Avira Free Antivirus

Manuale utente

Marchio registrato e copyright

Marchio registrato

Windows è un marchio registrato di Microsoft Corporation negli Stati Uniti e in altri paesi.
Tutti gli altri marchi o nomi di prodotti sono marchi registrati del legittimo proprietario.
I marchi protetti non sono contrassegnati come tali in questo manuale. Ciò tuttavia non significa che possano essere liberamente utilizzati.

Note sul Copyright

Per Avira Free Antivirus viene utilizzato codice di terzi. Ringraziamo i possessori di copyright per aver messo a disposizione il proprio codice.
Informazioni dettagliate sul copyright sono disponibili nella guida del programma di Avira Free Antivirus in "Third Party Licenses".

Indice

1. Introduzione

Il prodotto Avira protegge efficacemente il computer da virus, worm, trojan, adware, spyware e altri pericoli. In questo manuale vengono brevemente descritti virus o malware (software dannoso) e programmi indesiderati.

La guida descrive l'installazione e il funzionamento del programma.

Sul sito Web Avira sono disponibili numerose opzioni e ulteriori informazioni:

http://www.avira.it/free-av

Sul sito Web Avira è possibile:

- richiamare informazioni su ulteriori programmi Avira Desktop
- scaricare il programma Avira Desktop più recente
- scaricare il manuale del prodotto più recente in formato PDF
- scaricare strumenti di supporto e riparazione gratuiti
- utilizzare la banca dati completa e gli articoli FAQ relativi alla risoluzione di problemi
- richiamare gli indirizzi di assistenza specifici per paese.

Il team di Avira

1.1 Simboli ed evidenziazioni

Si utilizzano i seguenti simboli:

Simbolo/Definizione	Spiegazione
✓	Esiste un requisito che deve essere soddisfatto prima che sia eseguita un'operazione.
▸	Prima di un'operazione che deve essere eseguita dall'utente.
→	Prima di un evento scaturito dall'operazione precedente.
Attenzione	Prima di un avviso di pericolo di una significativa perdita di dati.

Suggerimenti	Prima di un messaggio con informazioni particolarmente importanti o prima di un suggerimento che agevola la comprensione e l'uso del prodotto Avira.

Si utilizzano le seguenti evidenziazioni:

Evidenziazione	Spiegazione
Corsivo	Nome del file o percorso.
	Elementi dell'interfaccia del software che vengono visualizzati (ad esempio sezione della finestra o avviso di errore).
Grassetto	Elementi dell'interfaccia software su cui è possibile fare clic (ad esempio voci di menu, rubriche, campi di opzione o pulsanti).

2. Informazioni sul prodotto

2.1 Panoramica

In questo capitolo è possibile ricevere tutte le informazioni importanti per l'acquisto e l'utilizzo del prodotto Avira:

- vedere capitolo: Prestazioni
- vedere capitolo: Requisiti di sistema
- vedere capitolo: Licenza e aggiornamento

I prodotti Avira offrono strumenti completi e flessibili per proteggere efficacemente il computer da virus, malware, programmi indesiderati e altri pericoli.

- Si noti:

Attenzione
La perdita di dati importanti ha spesso conseguenze drammatiche. Nemmeno il miglior programma antivirus può offrire una protezione al 100% contro la perdita di dati. Si consiglia di eseguire regolarmente copie di sicurezza (backup) dei dati.

Suggerimenti
Un programma in grado di proteggere il computer da virus, malware, programmi indesiderati e altri pericoli può essere affidabile ed efficace solo se aggiornato regolarmente. Si consiglia di garantire l'aggiornamento del prodotto Avira tramite aggiornamenti automatici. Configurare adeguatamente il programma.

2.2 Prestazioni

Il prodotto Avira dispone delle seguenti funzioni:

- Control Center per il monitoraggio, l'amministrazione e la gestione dell'intero programma
- Configurazione centrale con configurazione semplice in modalità esperto oppure standard e dotata di guida in linea sensibile al contesto
- System Scanner (On-Demand Scan) con scansione di tutti i tipi noti di virus e malware gestita da profilo e configurabile.
- Integrazione nella funzionalità di controllo di Windows Vista (Controllo dell'account utente) per poter eseguire operazioni per le quali sono necessari i diritti di amministratore.

- Realtime Protection (On-Access Scan) per il costante monitoraggio di tutti gli accessi ai file
- Avira SearchFree Toolbar (powered by Ask.com), una barra di ricerca integrata nel browser Web con la quale è possibile effettuare ricerche in internet in modo veloce e pratico.
- Per gli utenti di Avira Free Antivirus solo insieme a Avira SearchFree Toolbar: Web Protection per il monitoraggio dei dati e dei file trasferiti da Internet mediante protocollo HTTP (monitoraggio delle porte 80, 8080, 3128)
- Gestione integrata della quarantena per l'isolamento e il trattamento di file sospetti
- Rootkits Protection per il rilevamento di malware installatisi occultamente nel sistema del computer (i cosiddetti rootkit (non disponibile in Windows XP 64 Bit)
- Accesso diretto in Internet a informazioni dettagliate su virus rilevati e malware
- Aggiornamento semplice e rapido del programma, delle definizioni dei virus (VDF) e del motore di ricerca mediante Aggiornamento singolo file e aggiornamento incrementale VDF mediante un server web su Internet
- integrato per la pianificazione di operazioni singole o ricorrenti come aggiornamenti o scansioni
- Identificazione estremamente precisa di virus e malware per mezzo di tecnologie di ricerca (motore di ricerca) che includono la procedura di ricerca euristica
- Identificazione di tutti i tipi di archivio convenzionali, inclusa l'identificazione di archivi nascosti e Smart-Extension
- Elevata performance grazie alla capacità multi threading (scansione contemporanea di molti file ad alta velocità)

2.3 Requisiti di sistema

È necessario soddisfare i seguenti requisiti di sistema:

- Computer a partire dal Pentium, minimo 1 GHz
- Sistema operativo
  - Windows XP, SP3 (32 o 64 Bit) o
  - Windows Vista (32 o 64 Bit, SP1 consigliato) o
  - Windows 7 (32 o 64 Bit)
- Min. 150 MB di memoria libera sull'hard disk (maggiore quantità di memoria se si utilizza la quarantena e la memoria temporanea)
- Min. 512 MB di memoria principale in Windows XP
- Min. 1024 MB di memoria principale in Windows Vista, Windows 7
- Per l'installazione del programma: diritti di amministratore
- Per tutte le installazioni: Windows Internet Explorer 6.0 o superiore
- Eventuale connessione Internet (vedi Installazione)

Avira SearchFree Toolbar

- Sistema operativo
  - Windows XP, SP3 (32 o 64 Bit) o
  - Windows Vista (32 o 64 Bit, SP 1)
  - Windows 7 (32 o 64 Bit)
- Browser Web
  - Windows Internet Explorer 6.0 o superiore o
  - Mozilla Firefox 3.0 o superiore

> **Suggerimenti**
> Disinstallare barre di ricerca, se installate in precedenza, prima di installare Avira SearchFree Toolbar. In caso contrario non è possibile installare Avira SearchFree Toolbar.

Note per l'utente di Windows Vista

In Windows XP molti utenti lavorano con i diritti di amministratore. Tuttavia questo non è auspicabile dal punto di vista della sicurezza, poiché così anche i virus e i programmi indesiderati hanno la possibilità di infiltrarsi nel computer.

Per questo motivo Microsoft ha aggiunto in Windows Vista il "Controllo utente" (User Account Control). Esso offre una maggiore protezione per gli utenti che sono registrati come amministratori: l'amministratore quindi dispone in Windows Vista inizialmente solo dei privilegi di un utente normale. Le azioni per le quali sono necessari i diritti di amministratore sono chiaramente segnalate da Windows Vista con un'icona. Inoltre l'utente deve esplicitamente confermare l'azione desiderata. Dopo aver ricevuto l'approvazione, si registra un aumento dei privilegi e il sistema operativo esegue i propri compiti amministrativi.

Il prodotto Avira necessita dei diritti di amministratore per eseguire alcune azioni in Windows Vista. Queste azioni sono contrassegnate con il seguente carattere: . Se questo carattere appare su un pulsante, significa che sono necessari i diritti di amministratore per l'esecuzione di tale azione. Se l'attuale utente non dispone di tali diritti, Windows Vista propone una finestra di dialogo del Controllo Utente (User Account Control) per l'inserimento della password dell'amministratore. Se non si dispone di tale password, non è possibile eseguire questa azione.

2.4 Licenza e aggiornamento

Per poter utilizzare il prodotto Avira è necessario possedere una licenza. In questo modo si prende visione delle condizioni di licenza.

La licenza viene assegnata sotto forma di una chiave di attivazione. La chiave di attivazione è un codice alfanumerico che l'utente riceve all'acquisto del prodotto Avira. La chiave di attivazione comprende i dati esatti della licenza, ossia quali sono i programmi dotati di licenza e per quale periodo.

Se il prodotto Avira è stato acquistato in Internet, l'utente riceverà la chiave di attivazione per email, altrimenti è riportata sulla confezione del prodotto.

Per attivare la licenza del programma, è necessario immettere tale chiave durante l'attivazione del programma. L'attivazione del prodotto può avvenire durante l'installazione. Tuttavia, è possibile attivare il prodotto Avira anche in seguito nel Sistema di gestione delle licenze in Guida in linea > Sistema di gestione delle licenze.

In Avira Free Antivirus è già contenuta una chiave di attivazione valida. In questo modo si evita la procedura di attivazione del prodotto.

Nel Sistema di gestione delle licenze è possibile avviare un aggiornamento a un prodotto della famiglia Avira Desktop: In questo modo non è necessario disinstallare il vecchio prodotto manualmente e installare manualmente il nuovo. Tramite l'aggiornamento dal Sistema di gestione delle licenze immettere nell'apposito campo la chiave di attivazione del prodotto di cui si desidera effettuare l'aggiornamento. Il nuovo prodotto viene installato automaticamente.

Per raggiungere alta affidabilità e sicurezza per il computer, Avira rammenta all'utente di eseguire l'aggiornamento all'ultima versione. Fare clic su **Upgrade** nell'elemento pop-up per la migrazione all'ultima versione e l'utente verrà inoltrato alla pagina di aggiornamento specifica del prodotto. È possibile eseguire un aggiornamento per il prodotto attuale o acquistare un prodotto dall'ampia gamma di prodotti Avira. La pagina panoramica dei prodotti Avira mostra quale prodotto viene utilizzato attualmente e offre la possibilità di confrontarlo con altri prodotti Avira. Per ulteriori informazioni, fare clic sul simbolo delle informazioni a destra accanto al nome del prodotto. Se si desidera continuare ad usare il prodotto utilizzato finora, fare clic su **Upgrade** per installare subito l'ultima versione con le funzioni migliorate. Se si desidera acquistare un prodotto dell'ampia gamma, fare clic su **Acquista** in fondo alla colonna del prodotto corrispondente. Si viene reindirizzati al Negozio online di Avira per eseguire l'ordinazione.

> **Suggerimenti**
> A seconda del prodotto e del sistema operativo, è necessario possedere eventualmente i diritti di amministratore per eseguire l'aggiornamento. Registrarsi come amministratore e installare l'ultima versione.

È possibile effettuare l'aggiornamento dei seguenti prodotti:

- Aggiornamento di Avira AntiVir Personal ad Avira Free Antivirus.
- Aggiornamento di Avira AntiVir Personal ad Avira Antivirus Premium 2012.
- Aggiornamento da Avira AntiVir Premium ad Avira Internet Security 2012.

- Aggiornamento da Avira AntiVir Premium Security Suite ad Avira Professional Security.

3. Installazione e disinstallazione

3.1 Panoramica

In questo capitolo si ottengono informazioni relative all'installazione e la disinstallazione del prodotto Avira:

- vedere capitolo: Prima dell'installazione premesse, preparazione del computer all'installazione
- vedere capitolo: Installazione Express: installazione standard in base alle impostazioni predefinite
- vedere capitolo: Installazione personalizzata: installazione configurabile
- vedere capitolo: Assistente di configurazione
- vedere capitolo: Modifiche all'installazione
- vedere capitolo: Moduli di installazione
- vedere capitolo: Disinstallazione: esegui disinstallazione

3.1.1 Modi di installazione

Durante l'installazione mediante l'assistente di installazione è possibile selezionare un tipo di setup:

Express

- I file del programma vengono installati in una directory standard predefinita in *C:\Programmi*.
- Il prodotto Avira verrà installato con le impostazioni standard. È possibile effettuare impostazioni predefinite nell'assistente di configurazione.

Personalizzata

- È possibile selezionare per l'installazione singoli componenti del programma (vedere capitolo Installazione e disinstallazione > Moduli di installazione).
- Si può scegliere una cartella di destinazione per i file di programma da installare.
- È possibile stabilire se creare o meno un collegamento sul desktop e/o un gruppo di programmi sul menu di avvio.
- Con la configurazione guidata è possibile effettuare impostazioni personalizzate del prodotto Avira e indurre una breve scansione del sistema direttamente dopo l'installazione.

3.2 Prima dell'installazione

Suggerimenti
Prima dell'installazione verificare che il computer soddisfi i requisiti di sistema. Se il computer soddisfa tutti i requisiti minimi, è possibile installare il prodotto Avira.

Suggerimenti
Nell'installazione su un sistema operativo server, Realtime Protection e Protezione file non sono disponibili.

Inizializzazione prima dell'installazione

- ✓ Chiudere il programma email. Si consiglia inoltre di chiudere tutte le applicazioni in uso.
- ✓ Assicurarsi che non siano installate altre protezioni contro virus. Le funzioni automatiche di protezione di diverse applicazioni antivirus potrebbero entrare in conflitto.
  - ↳ Il prodotto Avira scansionerà il computer per controllare l'eventuale presenza di software incompatibili.
  - ↳ In caso di rilevamento di software incompatibile viene generato un elenco corrispondete di questi programmi.
  - ↳ Si consiglia di disinstallare il software che espone a rischi la sicurezza del computer.
- Scegliere dall'elenco quei programmi, che devono essere eliminati dal computer automaticamente, quindi fare clic su **Continua**.
- Alcuni programmi possono essere eliminati dal computer solo manualmente. Selezionare i programmi e fare clic su **Continua**.
  - ↳ La disinstallazione di uno o più programmi richiede il riavvio del computer. Dopo il riavvio, l’installazione continua.

Attenzione
Finché la procedura di installazione del prodotto Avira non è conclusa, il computer non è protetto.

Installazione

Il programma di installazione funziona in modalità di dialogo. Nella maggior parte dei passaggi di installazione è sufficiente fare un semplice clic per continuare.

I pulsanti principali hanno le seguenti funzioni:

- **OK**: per confermare l'azione.
- **Annulla**: per annullare l'azione.
- **Continua**: per passare alla fase successiva.
- **Indietro**: per passare alla fase precedente.

▸ Stabilire una connessione Internet. La connessione a Internet è necessaria per eseguire i seguenti passaggi dell'installazione:

  - Scaricare i file attuali di programma e del motore di ricerca, nonché i file di definizione dei virus aggiornati mediante il programma di installazione (per installazione basata su Internet)
  - Registrazione come utente
  - Esecuzione di un eventuale aggiornamento a installazione conclusa

▸ Tenere a portata di mano la chiave di licenza del prodotto Avira, se si desidera attivarlo.

Suggerimenti
Installazione basata su Internet:
per eseguire un'installazione basata su Internet del programma, è disponibile un programma di installazione che carica i file di programma aggiornati prima di eseguire l'installazione dai server Web di Avira. Tale procedura garantisce l'installazione di prodotto Avira con un file di definizione dei virus aggiornato.

Installazione con un pacchetto di installazione:
il pacchetto di installazione contiene sia il programma di installazione sia tutti i file di programma necessari. Tuttavia nell'installazione con un pacchetto di installazione non è possibile effettuare la selezione della lingua per il prodotto Avira. Al termine dell'installazione si consiglia di eseguire un aggiornamento del file di definizione dei virus.

Suggerimenti
Per la registrazione, il prodotto Avira comunica tramite il protocollo HTTP e la porta 80 (comunicazione Web), nonché tramite il protocollo di codifica SSL e la porta 443 con i server di Avira. Se si utilizza un firewall, assicurarsi che la connessione necessaria e i dati in entrata e in uscita non vengano bloccati dal firewall.

3.3 Installazione Express

Installare il prodotto Avira nel modo seguente:

Avviare il programma di installazione facendo doppio clic sul file di installazione scaricato da Internet o inserire il CD del programma.

Installazione basata su Internet

↳ Appare la finestra di dialogo **Benvenuti**.

- Fare clic su **Avanti** per continuare l'installazione.

↳ Appare la finestra di dialogo **Seleziona lingua**.

- Selezionare la lingua con cui si desidera installare il prodotto Avira e confermare la scelta con **Continua**.

↳ Appare la finestra di dialogo **Download**. Tutti i file necessari per l'installazione vengono scaricati dai server Web di Avira. Al termine del download la finestra **Download** si chiude.

Installazione con un pacchetto di installazione

↳ Viene visualizzata la finestra **Preparazione dell'installazione in corso**.

↳ Il file di installazione viene decompresso. La routine di installazione viene avviata.

↳ Appare la finestra di dialogo**Selezionare modalità di installazione**.

Suggerimenti
L'**Installazione Express**, durante la quale i componenti standard vengono installati senza possibilità di configurazione, è preimpostata come default. Per eseguire una **installazione personalizzata**, continuare a leggere qui di seguito: Installazione > Installazione personalizzata.

- Confermare **l'accettazione dei termini del contratto di licenza con l'utente finale**e **l'accettazione dell'accordo di uso privato**. Se si desidera leggere i dettagli dei contratti di licenza, fare clic sul link corrispondente.
- Fare clic su **Avanti**.

↳ Appare la finestra di dialogo **Avira SearchFree Toolbar più Protezione web (powered by Ask.com)**.

- Se si desidera installare Avira SearchFree Toolbar, confermare che si accettano le condizioni del**contratto di licenza di Ask.com** e che si desidera installare Web Protection con Avira SearchFree Toolbar.

Suggerimenti
Disinstallare barre di ricerca, se installate in precedenza, prima di installare Avira SearchFree Toolbar. In caso contrario non è possibile installare Avira SearchFree Toolbar.

- Attivare eventualmente l'opzione **Imposta Ask.com come motore di ricerca standard** e fare clic su **Continua**.
  - ↳ L'*assistente per l'installazione della licenza* si apre e aiuta l'utente nell'attivazione del programma.
  - ↳ A questo punto si ha la possibilità di configurare un server proxy.
  - ↳ Se è già stato ricevuto un codice di attivazione, selezionare **Attiva il prodotto**.
  - ↳ L'avanzamento dell'installazione viene visualizzato tramite una barra verde.
  - ↳ Fare clic su **Fine** per terminare il setup e uscire dal programma di installazione.
  - ↳ L'Icona Tray di Avira si trova nella barra delle applicazioni.
  - ↳ Il modulo **Updater** ricerca gli eventuali aggiornamenti disponibili per proteggere in modo ottimale il computer.
  - ↳ La finestra sullo stato di**Luke Filewalker** si apre con una prima ricerca diretta del sistema di scansione e informa l'utente circa lo stato della scansione visualizzandone i risultati.
- Se dopo la scansione del sistema viene richiesto di riavviare il sistema, eseguire tale operazione per consentire la protezione completa del sistema stesso.

Se l'installazione è avvenuta con successo, si consiglia di verificare lo stato di aggiornamento del programma di protezione nella sezione **Stato** del Control Center.

- Se il prodotto Avira visualizza un messaggio ad indicare che il computer non è completamente protetto, fare clic su **Risoluzione del problema**.
  - ↳ Compare la finestra di dialogo **Ripristina la protezione**.
- Massimizzare la sicurezza del sistema in uso attivando le opzioni prestabilite.
- Infine, è possibile eventualmente eseguire una scansione completa del sistema.

3.4 Installazione personalizzata

Installare il prodotto Avira nel modo seguente:

Avviare il programma di installazione facendo doppio clic sul file di installazione scaricato da Internet o inserire il CD del programma.

Installazione basata su Internet

  - ↳ Appare la finestra di dialogo **Benvenuti**.
- Fare clic su **Avanti** per continuare l'installazione.
  - ↳ Appare la finestra di dialogo **Seleziona lingua**.
- Selezionare la lingua con cui si desidera installare il prodotto Avira e confermare la scelta con **Continua**.

↳ Appare la finestra di dialogo **Download**. Tutti i file necessari per l'installazione vengono scaricati dai server Web di Avira. Al termine del download la finestra **Download** si chiude.

Installazione con un pacchetto di installazione

↳ Viene visualizzata la finestra **Preparazione dell'installazione in corso**.

↳ Il file di installazione viene decompresso. La routine di installazione viene avviata.

↳ Appare la finestra di dialogo**Selezionare modalità di installazione**.

> **Suggerimenti**
> L'**Installazione Express**, durante la quale i componenti standard vengono installati senza possibilità di configurazione, è preimpostata come default. Se si desidera eseguire tale operazione, continuare a leggere qui di seguito: Installazione > Installazione Express.

- Come modalità di installazione desiderata selezionare **Personalizzata**.
- Confermare **l'accettazione dei termini del contratto di licenza con l'utente finale**e **l'accettazione dell'accordo di uso privato**. Se si desidera leggere i dettagli dei contratti di licenza, fare clic sul link corrispondente.
- Fare clic su **Avanti**.

  ↳ Appare la finestra di dialogo **Avira SearchFree Toolbar più Protezione web (powered by Ask.com)**.

- Se si desidera installare Avira SearchFree Toolbar, confermare che si accettano le condizioni del contratto di licenza di Ask.com e che si desidera installare Web Protection con Avira SearchFree Toolbar.

> **Suggerimento**
> Disinstallare eventuali barre di ricerca, se installate in precedenza, prima di installare Avira SearchFree Toolbar. In caso contrario non è possibile installare Avira SearchFree Toolbar.

- Attivare eventualmente l'opzione **Imposta Ask.com come motore di ricerca standard** e fare clic su **Continua**.

  ↳ Viene visualizzata la finestra **Seleziona directory di destinazione**.

  ↳ La directory preimpostata è *C:\Programmi\Avira\AntiVir Desktop*

- Fare clic su **Avanti** per continuare con l'installazione.

  - OPPURE -

  Selezionare mediante **Sfoglia** un'altra directory di destinazione e confermare con **Avanti**.

↳ Appare la finestra **Installa i componenti**:

- Attivare o disattivare i componenti desiderati e confermare con **Avanti**.

  ↳ Nelle seguenti finestre di dialogo è possibile stabilire se creare o meno un collegamento sul desktop e/o un gruppo di programmi sul menu.

- Fare clic su **Avanti**.

  ↳ Si apre l'assistente per l'installazione della licenza.

Nell'assistente per l'installazione della licenza è possibile registrarsi come cliente e abbonarsi alla *newsletter di Avira*. A tal fine è necessario immettere i propri dati personali.

- Inserire eventualmente i propri dati e confermarli con **Avanti**.

  ↳ Durante la registrazione, nella seguente finestra di dialogo viene visualizzato il risultato dell'attivazione.

- Fare clic su **Avanti**.

  ↳ I componenti del programma vengono installati. L'avanzamento dell'installazione viene visualizzato nella finestra di dialogo.

- Dopo la chiusura del processo di installazione, terminare quest'ultima con **Fine**.

  ↳ Si chiude l'assistente di installazione e si apre l'Assistente di configurazione.

3.5 Assistente di configurazione

Nell'installazione personalizzata, alla fine si apre l'assistente di configurazione. Quest'ultimo permette di effettuare importanti impostazioni predefinite per il prodotto Avira.

- Fare clic su **Avanti** nella finestra di benvenuto dell'assistente di configurazione per iniziare la configurazione del programma.

  ↳ Nella finestra di dialogo **Configura AHeAD** è possibile selezionare un livello di riconoscimento per la tecnologia AHeAD. Il livello di riconoscimento selezionato viene registrato per l'impostazione della tecnologia AHeAD di System Scanner (scansione diretta) e di Realtime Protection (scansione in tempo reale).

- Selezionare un livello di riconoscimento e proseguire la configurazione con **Avanti**.

  ↳ Nella finestra di dialogo seguente **Seleziona categorie estese delle minacce** è possibile adattare le funzioni di protezione del proprio prodotto Avira con la selezione delle categorie delle minacce.

- Attivare eventualmente ulteriori categorie delle minacce e proseguire la configurazione con **Avanti**.

  ↳ Nel caso in cui si sia selezionato il modulo di installazione Avira Realtime Protection, compare la finestra di dialogo **Modalità di avvio di Realtime Protection**. È ora possibile stabilire il momento in cui avviare Realtime Protection. Nella modalità di avvio indicata, Realtime Protection viene avviato a ogni riavvio del computer.

Suggerimenti
La modalità di avvio indicata di Realtime Protection viene memorizzata nel registro e non può essere modificata mediante la configurazione.

Suggerimenti
Al momento dell'avvio del computer, un'eventuale conseguenza della selezione della modalità di avvio di default per Realtime Protection (avvio normale) e di un rapido accesso all'account utente può essere la mancata scansione dei programmi che si avviano automaticamente all'avvio del sistema, dal momento che essi vengono avviati prima del completo caricamento di Realtime Protection.

- Attivare l'opzione desiderata e proseguire la configurazione con **Avanti**.
  - ↳ Nella finestra di dialogo seguente **Scansione del sistema** è possibile attivare o disattivare l'esecuzione di una scansione rapida del sistema. La scansione rapida del sistema viene eseguita al termine della configurazione e prima di riavviare il computer, e verifica la presenza di virus e malware nei programmi avviati e nei file di sistema più importanti.
- Attivare o disattivare l'opzione **Scansione rapida del sistema** e proseguire la configurazione con **Avanti**.
  - ↳ Nella finestra di dialogo seguente è possibile terminare la configurazione con **Fine**.
  - ↳ Le impostazioni indicate e selezionate vengono registrate.
  - ↳ Se è attivata l'opzione **Scansione rapida del sistema**, si apre la finestra **Luke Filewalker**. System Scanner esegue una scansione rapida del sistema.
  - ↳ Se dopo la scansione del sistema viene richiesto di riavviare il sistema, eseguire tale operazione per consentire la protezione completa del sistema stesso.

Se l'installazione è avvenuta con successo, si consiglia di verificare lo stato di aggiornamento del programma di protezione nella sezione **Stato** del Control Center.

- Se il prodotto Avira visualizza un messaggio ad indicare che il computer non è completamente protetto, fare clic su **Risoluzione del problema**.
  - ↳ Compare la finestra di dialogo **Ripristina la protezione**.
- Massimizzare la sicurezza del sistema in uso attivando le opzioni prestabilite.
- Infine, è possibile eventualmente eseguire una scansione completa del sistema.

3.6 Modifiche all'installazione

È possibile aggiungere o eliminare singoli componenti del programma all'attuale installazione del prodotto Avira (vedere Capitolo Installazione e disinstallazione > Moduli d'installazione)

Se si desidera aggiungere o eliminare componenti del programma dell'installazione corrente, è possibile utilizzare l'opzione **Installazione applicazioni**, **Cambia/Rimuovi programmi** all'interno del **pannello di controllo di Windows**.

Selezionare il prodotto Avira desiderato e fare clic su **Modifica**. Nella finestra di dialogo di *benvenuto* del programma selezionare l'opzione **Modifica programma**. Si è così inseriti nella modifica dell'installazione.

> **Suggerimenti**
> Quando si disinstalla Avira SearchFree Toolbar, viene disinstallato anche Web Protection.

3.7 Moduli di installazione

Nel caso di un'installazione personalizzata o di una modifica di un'installazione è possibile selezionare, aggiungere o eliminare i seguenti moduli:

- **Avira Free Antivirus**
  Questo modulo contiene tutti i componenti necessari per l'installazione corretta del prodotto Avira.
- **Avira Realtime Protection**
  Realtime Protection di Avira è in esecuzione in background. Monitora e ripara i file, quando possibile, durante operazioni come apertura, scrittura e copia in tempo reale (On-Access = all'accesso). Se un utente esegue un'operazione (caricamento, esecuzione, copia di un file), il prodotto Avira scansiona automaticamente il file. Durante l'operazione di rinomina del file Realtime Protection di Avira non esegue alcuna scansione.
- **Avira Web Protection** (per gli utenti di Avira Free Antivirus solo insieme a Avira SearchFree Toolbar)
  Durante la navigazione in Internet si richiedono dati da un server Web mediante il browser Web. I dati trasferiti dal server Web (file HTML, file di script e immagini, file flash, file audio e video, ecc.) normalmente passano dalla cache del browser direttamente all'esecuzione nel browser Web cosicché non è possibile una scansione in tempo reale come quella prevista da Avira Realtime Protection. In questo modo virus e programmi indesiderati potrebbero entrare nel computer. Web Protection è un cosiddetto proxy HTTP che monitora le porte utilizzate per il trasferimento dei dati (80, 8080, 3128) e controlla la presenza di virus e programmi indesiderati nei file trasferiti. In base alla configurazione il programma tratta i file infetti automaticamente o chiede all'utente l'azione da eseguire.

- **Avira Rootkits Protection**
  Avira Rootkits Protection controlla se sul computer sono già installati programmi software che dopo l'intrusione nel computer non si riesce a rilevare con i metodi convenzionali del riconoscimento di malware.
- **Shell Extension**
  L'estensione shell crea nel menu contestuale di Windows Explorer (tasto destro del mouse) la voce *Controlla i file selezionati con Avira*. Con questa voce è possibile scansionare direttamente singoli file o directory.

3.8 Disinstallazione

Se si desidera eliminare il prodotto Avira dal proprio computer, è possibile utilizzare l'opzione **Software** per cambiare o rimuovere i programmi (**Cambia/Rimuovi**) nel pannello di controllo di Windows.

È possibile disinstallare il prodotto Avira (descritto ad esempio per Windows XP e Windows Vista) nel seguente modo:

- Aprire nel menu **Start** di Windows il **Pannello di controllo**.
- Fare doppio clic su **Programmi** (Windows XP: **Software**).
- Selezionare il prodotto Avira desiderato dall'elenco e fare clic su **Rimuovi/Disinstalla**.
  - ↳ Verrà chiesto all'utente se desidera davvero eliminare il programma.
- Confermare con **Sì**.
  - ↳ Tutte le componenti del programma vengono eliminate.
- Fare clic su **Fine** per terminare la disinstallazione.
  - ↳ Appare una finestra di dialogo con il suggerimento di riavviare il computer.
- Confermare con **Sì**.
  - ↳ Il prodotto Avira viene quindi disinstallato, se necessario il computer viene riavviato e tutte le directory, i file e le voci del registro del programma vengono eliminate.

> **Suggerimenti**
> L'Avira SearchFree Toolbar non viene disinstallata con il programma; essa deve essere infatti disinstallata separatamente tramite i suddetti passaggi. Per fare questo è necessario attivare l'Avira SearchFree Toolbar tramite l'Add-On Manager in Firefox (non valido per Internet Explorer). Al termine della disinstallazione, la barra di ricerca non è più integrata nel browser.

Suggerimento
Quando si disinstalla Avira SearchFree Toolbar, viene disinstallato anche Web Protection.

4. Panoramica

In questo capitolo è possibile consultare una panoramica delle funzionalità e del funzionamento del prodotto Avira.

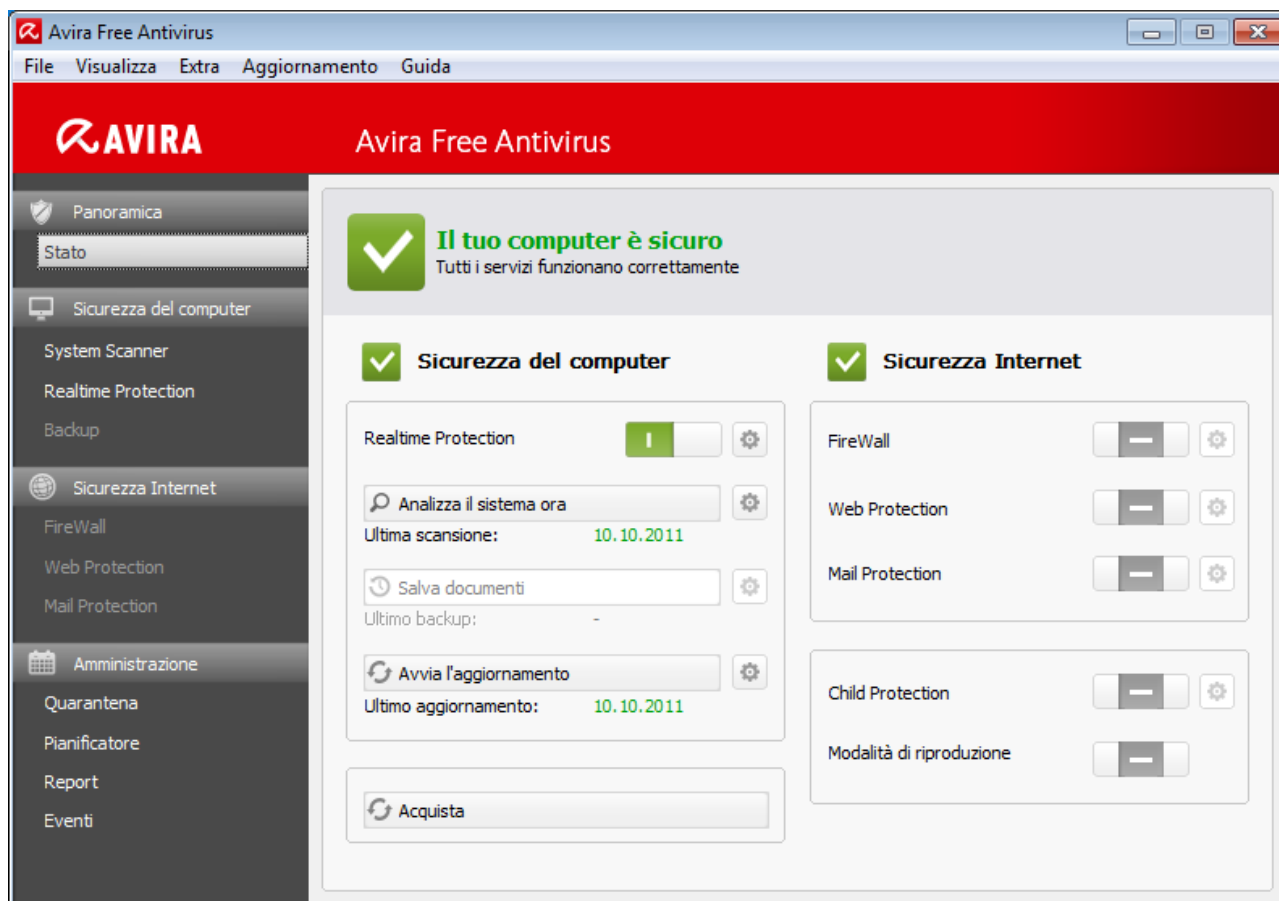
- vedere capitolo Interfaccia e funzionamento
- Vedere capitolo Toolbar
- vedere capitolo Come procedere

4.1 Interfaccia utente e funzionamento

È possibile usare il prodotto Avira mediante tre elementi dell'interfaccia del programma:

- Control Center: monitoraggio e gestione del prodotto Avira
- Configurazione: configurazione del prodotto Avira
- Icona Tray della barra delle applicazioni: Apertura di Control Center e altre funzioni

4.1.1 Control Center

Il Control Center serve per il monitoraggio dello stato di protezione del computer e per la gestione e il funzionamento delle componenti di protezione e delle funzioni del prodotto Avira.

La finestra del Control Center è divisa in tre sezioni: l'**elenco menu**, la **barra di navigazione** e la finestra per i dettagli **Stato**:

- **Elenco menu:** nei menu del Control Center è possibile richiamare funzioni generali del programma e informazioni sul prodotto.
- **Sezione di navigazione:** nella sezione di navigazione è possibile passare in modo semplice da una rubrica all'altra del Control Center. Le singole rubriche contengono informazioni e funzioni delle componenti del programma e sono presenti sulla barra di navigazione in base alle sezioni dei task. Esempio: sezione dei task **Sicurezza del computer** - Rubrica **Realtime Protection**.
- **Stato:** La schermata di avvio Stato consente in modo immediato di verificare se il computer è sufficientemente protetto e di avere una panoramica dei moduli attivi e del momento in cui sono stati eseguiti l'ultimo backup e l'ultima scansione di sistema. Nella finestra **Stato** si trovano i pulsanti per l'esecuzione di funzioni o azioni, come ad esempio l'attivazione o la disattivazione del servizio Child Protection.

Avvio e chiusura di Control Center

Per avviare Control Center è possibile scegliere tra le seguenti modalità:

- fare doppio clic sull'icona del programma sul desktop
- mediante la voce nel menu **Start > Programmi**.
- mediante l'Icona Tray del prodotto Avira

Si può chiudere il Control Center mediante il comando **Chiudi** nel menu **File**, con la shortcut **Alt+F4** o facendo clic sulla x nella finestra di Control Center.

Utilizzo di Control Center

Come navigare nel Control Center:

- Nella barra di navigazione fare clic su una sezione dei task sotto una rubrica.
  - ↳ La sezione dei task viene visualizzata nella finestra per i dettagli con ulteriori possibilità relative a funzionalità e configurazioni.
- Fare clic su un'altra sezione dei task per visualizzarla nella finestra per i dettagli.

> **Suggerimenti**
> Attivare la navigazione da tastiera nell'elenco menu con l'ausilio del tasto [**Alt**]. Con il tasto **Invio** si attiva la voce di menu selezionata in quel momento. Per aprire, chiudere o navigare nei menu del Control Center, è possibile utilizzare anche le combinazioni di tasti: tasto [**Alt**] + lettera sottolineata nel menu o nel comando. Tenere premuto il tasto [**Alt**] se si desidera richiamare un comando o un sottomenu dal menu.

Come elaborare dati o oggetti che vengono visualizzati nella finestra dei dettagli:

- Evidenziare i dati o gli oggetti che si desidera elaborare.

  Per evidenziare più elementi, tenere premuto il tasto **Ctrl** o il tasto **Shift** (selezione di elementi consecutivi) durante la selezione degli elementi.
- Fare clic sui pulsanti desiderati nella barra superiore della finestra dei dettagli per elaborare l'oggetto.

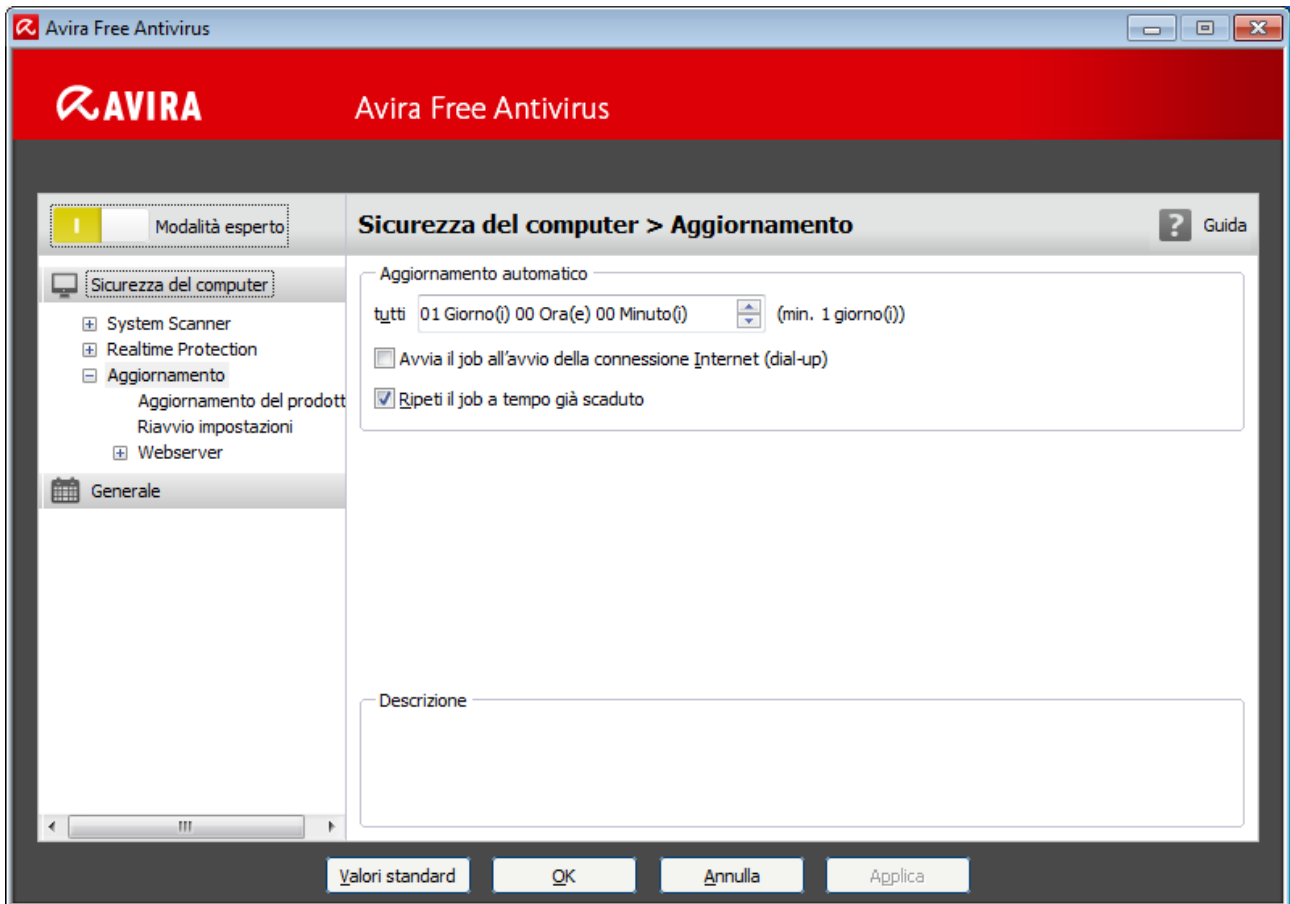
Control Center in sintesi

- **Stato**: nella schermata di avvio **Stato** sono disponibili tutte le rubriche che consentono di monitorare le funzionalità del prodotto Avira.
  - La finestra **Stato** offre la possibilità di visualizzare immediatamente quali moduli del programma sono attivi e fornisce informazioni sull'ultimo aggiornamento effettuato.Inoltre, è possibile verificare se si possiede una licenza valida.
- **Sicurezza del computer**: in **Sicurezza del computer** sono disponibili i componenti con cui eseguire la ricerca di virus e malware nei file del computer.
  - La rubrica System Scanner offre la possibilità di configurare o avviare la scansione diretta in modo semplice. I profili predefiniti consentono una scansione con le opzioni standard già adeguate. Con l'aiuto della Selezione manuale (non viene memorizzata) è possibile adattare la scansione di virus e programmi indesiderati alle proprie esigenze personali.
  - La rubrica Realtime Protection visualizza informazioni su file scansionati, così come ulteriori dati statistici, che possono essere ripristinati in qualsiasi momento e

permette il richiamo del file di report. Informazioni dettagliate sull'ultimo virus o programma indesiderato trovato sono reperibili "premendo un pulsante".

- **Sicurezza Internet**: in **Sicurezza Internet** sono disponibili i componenti che consentono di proteggere il computer da virus e malware provenienti da Internet, nonché da accessi di rete indesiderati.
  - La rubrica Web Protection visualizza informazioni sugli URL scansionati e sui virus individuati, nonché ulteriori dati statistici che possono essere ripristinati in qualsiasi momento, e consente di richiamare il file di report. Informazioni dettagliate sull'ultimo virus o programma indesiderato trovato sono reperibili "premendo un pulsante".
- **Gestione**: in **Gestione** sono disponibili gli strumenti che consentono di isolare e gestire file sospetti o infetti, nonché di pianificare attività ricorrenti.
  - Nella rubrica Quarantena è disponibile il cosiddetto Gestore della quarantena: la postazione centrale per i file già in quarantena o per file sospetti che si desidera spostare in quarantena. Inoltre esiste la possibilità di inviare un file selezionato per email all'Avira Malware Research Center.
  - La rubrica Scheduler offre la possibilità di creare sia job temporizzati di controllo e di aggiornamento che job, nonché di cancellare o modificare job esistenti.
  - La rubrica Report consente di visualizzare i risultati delle azioni eseguite.
  - La rubrica Eventi consente di ottenere informazioni sugli eventi generati dai moduli del programma.

4.1.2 Configurazione

In Configurazione è possibile effettuare le impostazioni per il prodotto Avira. Dopo l'installazione, il prodotto Avira è configurato con le impostazioni standard che assicurano la protezione ottimale del computer. Ciononostante, il computer o le richieste dell'utente per il prodotto Avira possono possedere caratteristiche particolari e richiedere un adattamento delle componenti di protezione del programma.

La configurazione dispone di una finestra di dialogo: con il pulsante **OK** o **Applica** si memorizzano le impostazioni scelte durante la configurazione, con **Annulla** si rifiutano le impostazioni, con il pulsante **Valori standard** è possibile ripristinare le impostazioni dei valori standard della configurazione. Nella barra di navigazione a sinistra è possibile selezionare singole rubriche di configurazione.

Richiamo della Configurazione

Esistono diverse possibilità per richiamare la configurazione:

- Mediante il Pannello di controllo di Windows.
- Mediante il centro sicurezza di Windows - a partire da Windows XP Service Pack 2.
- mediante l'Icona Tray del programma Avira.
- nel Control Center mediante la voce di menu Extra > Configurazione.
- Nel Control Center mediante il pulsante Configurazione.

Suggerimenti
Se si richiama la configurazione con il pulsante **Configurazione** in Control Center, si giunge nel registro di configurazione della categoria attiva in Control Center. Per selezionare un singolo registro di configurazione, è necessario

attivare la **Modalità esperto** della configurazione. In questo caso appare una finestra di dialogo, in cui viene richiesto di attivare la **Modalità esperto**.

Utilizzo della Configurazione

All'interno della finestra di configurazione si può navigare come in Esplora risorse di Windows:

- Fare clic su una voce della struttura ad albero per visualizzare questa categoria di configurazione nella finestra dei dettagli.
- Fare clic sul segno + prima delle voci per estendere la categoria di configurazione e visualizzare le rubriche di configurazione subordinate nella struttura ad albero.
- Per nascondere le rubriche di configurazione subordinate, fare clic sul segno - (meno) prima della categoria di configurazione estesa.

Suggerimenti
Per attivare o disattivare le opzioni nella configurazione e per premere i pulsanti è possibile utilizzare anche le seguenti combinazioni di tasti: tasto [**Alt**] + lettera sottolineata nei nomi opzione o nella definizione pulsanti.

Suggerimenti
Le rubriche di configurazione vengono visualizzate per intero nella modalità esperto. Attivare la **Modalità esperto** per visualizzare tutte le rubriche di configurazione. La **Modalità esperto** può essere protetta con una password da digitare al momento dell'attivazione.

Se si desidera registrare le impostazioni nella configurazione:

- Fare clic sul pulsante **OK**.

  ↬ La finestra di configurazione viene chiusa e le impostazioni registrate.

  - OPPURE -

  Fare clic sul pulsante **Applica**.

  ↬ Le impostazioni vengono registrate. La finestra di configurazione rimane aperta.

Se si desidera terminare la configurazione senza memorizzare le impostazioni:

- Fare clic sul pulsante **Annulla**.

  ↬ La finestra di configurazione si chiude e le impostazioni vengono ignorate.

Se si desidera ripristinare tutte le impostazioni dei valori standard nella configurazione:

- Fare clic su **Valori standard**.

↳ Tutte le impostazioni dei valori standard nella configurazione vengono ripristinate. Quando si ripristinano i valori standard tutte le modifiche e le immissioni dell'utente vengono perse.

Opzioni di configurazione in sintesi

Esistono le seguenti opzioni di configurazione:

- **System Scanner**: Configurazione della scansione diretta
  - Opzioni di ricerca
  - Azioni in caso di rilevamento
  - Opzioni per la scansione degli archivi
  - Eccezioni della scansione diretta
  - Euristica della scansione diretta
  - Impostazione della funzione di report
- **Realtime Protection**: Configurazione della scansione in tempo reale
  - Opzioni di ricerca
  - Azioni in caso di rilevamento
  - Eccezioni della scansione in tempo reale
  - Euristica della scansione in tempo reale
  - Impostazione della funzione di report
- **Web Protection**: configurazione del servizio Web Protection
  - Opzioni di ricerca, attivazione e disattivazione di Web Protection
  - Azioni in caso di rilevamento
  - Accesso bloccato: Filtro Web per URL noti indesiderati (malware, phishing ecc.)
  - Eccezioni della scansione di Web Protection: URL, tipi di dati, tipi di MIME
  - Euristica di Web Protection
  - Impostazione della funzione di report
- **Generale**:
  - Categorie estese delle minacce per la scansione diretta e in tempo reale
  - Sicurezza: indicatore di stato aggiornamento, indicatore di stato scansione completa del sistema, protezione del prodotto
  - WMI: attiva supporto WMI
  - Configurazione del log eventi
  - Configurazione delle funzioni di report
  - Impostazione delle directory utilizzate
  - Aggiornamento: configurazione del collegamento al server di download, impostazione dell'aggiornamento del prodotto
  - Configurazione degli avvisi acustici in caso di rilevamento malware

4.1.3 Icona Tray

Dopo l'installazione, l'icona Tray del prodotto Avira è collocata nella barra delle applicazioni:

Simbolo	Descrizione
	Realtime Protection di Avira
	Realtime Protection di Avira è disattivato

L'icona Tray mostra lo stato dei servizi Realtime Protection.

Le funzioni principali del prodotto Avira sono facilmente accessibili mediante il menu contestuale dell'icona Tray.

- Per richiamare il menu contestuale, fare clic con il tasto destro del mouse sull'icona Tray.

Voci del menu contestuale

- **Attivazione di Realtime Protection**: attiva o disattiva il servizio Realtime Protection di Avira.
- **Attivazione di Web Protection**: attiva o disattiva il servizio Web Protection di Avira.
- **Avvio**: apre il Control Center.
- **Configurazione di Avira**: apre la Configurazione.
- **Avvia aggiornamento**: avvia un aggiornamento.
- **Guida in linea**: Apre la Guida in linea.
- **Informazioni su Avira Free Antivirus:** apre una finestra di dialogo con informazioni sul prodotto Avira in uso: Informazioni su prodotto, versione e licenza.
- **Avira su Internet**: Apre il portale Web di Avira in Internet. Il prerequisito essenziale è l'accesso attivo a Internet.

4.2 Toolbar

4.2.1 Panoramica

Al termine di un'installazione terminata con successo, l'Avira SearchFree Toolbar è integrata nel browser Web. Alla prima apertura del browser si apre una finestra di stato contenente informazioni importanti sulle funzioni della toolbar.

La toolbar è formata da un campo di ricerca, un logo Avira collegato al sito Web aziendale, due display di stato e il menu **Opzioni**.

- Barra di ricerca
  Utilizzare la barra di ricerca per effettuare ricerche in Internet in modo veloce e gratuito tramite il motore di ricerca Ask.com.
- Display di stato
  I display di stato indicano lo stato di Web Protection e l'attuale stato di aggiornamento di prodotto Avira, aiutando l'utente a riconoscere quali azioni devono essere eseguite per proteggere il PC.
- Opzioni
  Tramite il menu Opzioni è possibile accedere alle Opzioni della toolbar, cancellare la cronologia delle ricerche, richiamare la Guida in linea e le Informazioni relative alla toolbar e disinstallare l'Avira SearchFree Toolbar direttamente tramite browser Web (solo per Firefox).

4.2.2 Utilizzo

Barra di ricerca

Tramite la barra di ricerca è possibile ricercare in internet uno o più termini.

Per fare questo inserire il termine desiderato nel campo di ricerca e premere poi il pulsante **Invio** o fare clic su **Cerca**. Il motore di ricerca Ask.com esegue la ricerca in internet e mostra poi tutti i risultati riscontrati nella finestra del browser.

La procedura per eseguire la configurazione personalizzata dell'Avira SearchFree Toolbar in Internet Explorer e Firefox è contenuta in **Opzioni.**

Display di stato

Web Protection

Web Protection è attivato.

Avira Web Protection è attivo e il PC è protetto.

Web Protection è disattivato.

Avira Web Protection è disattivato. Controllare l'applicazione e attivare Web Protection per avere la necessaria protezione.

Stato aggiornamento

Sulla destra si trova l'avviso di stato, che fornisce informazioni sullo stato di aggiornamento di Avira. Simboli e avvisi indicano quali azioni devono essere eventualmente eseguite a protezione del proprio PC.

Aggiornamento quotidiano finito.

Passando con il puntatore del mouse sul simbolo, appare il seguente avviso: *Avira è aggiornato e il PC è protetto.*

Non sono necessarie ulteriori azioni.

Aggiorna Avira.

Passando con il puntatore del mouse sul simbolo, appare il seguente avviso: *Avira non è aggiornato. Fai clic qui per scaricare l'ultimo aggiornamento e avere la protezione necessaria al PC.*

- Fare clic sul simbolo giallo o sul testo per aggiornare il prodotto Avira. La procedura avviene in base alle impostazioni predefinite fissate per Avira Free Antivirus.
  - ↳ Durante l'aggiornamento appare un avviso *Aggiornamento in corso...*
  - ↳ Al termine di un aggiornamento completato con successo viene di nuovo visualizzato il simbolo verde con l'avviso *Aggiornamento giornaliero eseguito*.

Avira non è disponibile.

Passando con il puntatore del mouse sul simbolo, appare il seguente avviso: *Avira non è disponibile. Per assicurarsi che la protezione sia presente, controllare se l'applicazione è ancora installata e viene eseguita.*

- Fare clic sul simbolo grigio o sul testo per collegarsi alla pagina di aiuto di Avira. Qui verranno fornite ulteriori informazioni su come procedere.

4.2.3 Opzioni

L'Avira SearchFree Toolbar è compatibile con Internet Explorer e Firefox e può essere configurata in entrambi i browser Web in base alle esigenze dell'utente.

- Opzioni di configurazione con Internet Explorer
- Opzioni di configurazione con Firefox

Internet Explorer

Nel browser Web Internet Explorer, nel menu **Opzioni** sono disponibili le seguenti opzioni di configurazione per l'Avira SearchFree Toolbar:

Opzioni della Toolbar

Cerca

Seleziona motore Ask

Nel menu **Seleziona motore Ask** è possibile selezionare quale motore di ricerca Ask deve essere utilizzato per la ricerca. Sono disponibili motori di ricerca delle seguenti zone: USA, Brasile, Germania, Spagna, Europa, Francia, Italia, Paesi Bassi, Russia e Gran Bretagna.

Avvia ricerche in

Nel menu dell'opzione **Avvia ricerche in** è possibile selezionare dove deve essere visualizzato il risultato di una ricerca, se nella **Finestra attiva**, in una **Nuova finestra** o su una **Nuova scheda**.

Mostra ultime ricerche

Se l'opzione **Mostra ultime ricerche** è attiva, sotto al campo di inserimento testo della barra di ricerca vengono visualizzati i termini di ricerca digitati fino a quel momento.

Azzera la cronologia delle ricerche all'uscita del browser

Attivare l'opzione **Azzera la cronologia delle ricerche all'uscita del browser**, quando non si vuole salvare la cronologia delle ricerche già effettuate e si desidera che venga cancellata alla chiusura del browser.

Altre opzioni

Seleziona lingua barra

In **Seleziona lingua barra** è possibile selezionare la lingua di Avira SearchFree Toolbar. Sono disponibili le versioni in inglese, tedesco, spagnolo, francese, italiano e portoghese.

> **Suggerimenti**
> La lingua preimpostata dell'Avira SearchFree Toolbar corrisponde a quella del programma dell'utente, se disponibile. Se la toolbar non è disponibile nella lingua dell'utente, viene preimpostata la lingua inglese.

Visualizza i nomi dei pulsanti

Disattivare l'opzione **Visualizza i nomi dei pulsanti**, se si desidera nascondere il testo accanto alle icone di Avira SearchFree Toolbar.

Azzera cronologia delle ricerche

Attivare l'opzione**Azzera cronologia delle ricerche**, se non si desidera salvare le ricerche già eseguite.

Guida in linea

Fare clic su **Guida in linea**, per richiamare la pagina Web con le domande frequenti (FAQ) riguardo la toolbar.

Disinstalla

È possibile disinstallare l'Avira SearchFree Toolbar anche direttamente in Internet Explorer: Disinstallazione mediante il browser Web.

Info

Fare clic su **Info**, per sapere quale versione di Avira SearchFree Toolbar è installata.

Firefox

Nel browser Web Firefox, nel menu **Opzioni** sono disponibili le seguenti opzioni di configurazione per l'Avira SearchFree Toolbar:

Opzioni della Toolbar

Cerca

Seleziona motore Ask

Nel menu Seleziona motore Ask è possibile selezionare quale motore di ricerca Ask deve essere utilizzato per la ricerca. Sono disponibili motori di ricerca delle seguenti zone: USA, Brasile, Germania, Spagna, Europa, Francia, Italia, Paesi Bassi, Russia e Gran Bretagna.

Mostra ultime ricerche

Se l'opzione Mostra ultime ricerche è attiva, è possibile visualizzare i termini di ricerca digitati fino a quel momento, facendo clic sulla freccia nella barra di ricerca. Selezionare uno dei termini se si vuole visualizzare nuovamente il risultato di tale ricerca.

Azzera la cronologia delle ricerche all'uscita del browser

Attivare l'opzione Azzera la cronologia delle ricerche all'uscita del browser, quando non si vuole salvare la cronologia delle ricerche già effettuate e si desidera che venga cancellata alla chiusura del browser.

Mostra i risultati della ricerca di Ask, quando vengono inseriti indirizzi URL non validi o parole chiave nel campo degli indirizzi del browser

Se questa opzione è attiva, ogni volta che parole chiave o indirizzi URL non validi vengono inseriti nel campo degli indirizzi del browser, viene avviata una ricerca e mostrati i relativi risultati.

Altre opzioni

Seleziona lingua barra

In **Seleziona lingua barra** è possibile selezionare la lingua di Avira SearchFree Toolbar. Sono disponibili le versioni in inglese, tedesco, spagnolo, francese, italiano e portoghese.

> **Suggerimenti**
> La lingua preimpostata dell'Avira SearchFree Toolbar corrisponde a quella del programma dell'utente, se disponibile. Se la toolbar non è disponibile nella lingua dell'utente, viene preimpostata la lingua inglese.

Visualizza i nomi dei pulsanti

Disattivare l'opzione **Visualizza i nomi dei pulsanti**, se si desidera nascondere il testo accanto alle icone di Avira SearchFree Toolbar.

Azzera cronologia delle ricerche

Facendo clic su **Azzera cronologia delle ricerche**, vengono cancellati tutti i termini ricercati con Avira SearchFree Toolbar fino a quel momento.

Guida in linea

Fare clic su **Guida in linea**, per richiamare la pagina Web con le domande frequenti (FAQ) riguardo la toolbar.

Disinstalla

È possibile disinstallare l'Avira SearchFree Toolbar anche direttamente in Firefox: Disinstallazione mediante il browser Web.

Info

Fare clic su **Info**, per sapere quale versione di Avira SearchFree Toolbar è installata.

4.2.4 Disinstallazione

Si può disinstallare Avira SearchFree Toolbar (descritto ad esempio per Windows XP e Windows Vista) nel seguente modo:

- Aprire nel menu **Start** di Windows il **Pannello di controllo**.
- Fare doppio clic su **Programmi** (Windows XP: **Software**).
- Selezionare **Avira SearchFree Toolbar plus Web Protection** nell'elenco e fare clic su **Cancella**.
  - ↳ Verrà chiesto all'utente se desidera davvero disinstallare il prodotto.
- Confermare con **Sì**.

↳ Avira SearchFree Toolbar plus Web Protection viene disinstallato, se necessario il computer viene riavviato e tutte le directory, i file e le voci del registro di Avira SearchFree Toolbar plus Web Protection vengono eliminate.

Disinstallazione mediante il browser Web

È inoltre possibile disinstallare l'Avira SearchFree Toolbar direttamente nel browser:

- aprire nella barra di ricerca a destra il menu **Opzioni**.
- Fare clic su **Disinstalla**.

  ↳ Viene richiesto di chiudere il browser Web, se ancora aperto.

- Chiudere il browser Web e fare clic su **OK**.

  ↳ Avira SearchFree Toolbar plus Web Protection viene disinstallato, se necessario il computer viene riavviato e tutte le directory, i file e le voci del registro di Avira SearchFree Toolbar plus Web Protection vengono eliminate.

Suggerimento
Quando si disinstalla Avira SearchFree Toolbar, viene disinstallato anche Web Protection.

Suggerimenti
Per disinstallare l'Avira SearchFree Toolbar da Firefox, il toolbar deve essere attivato in Add-On Manager.

4.3 Come procedere

4.3.1 Eseguire gli aggiornamenti automatici

Con la seguente procedura è possibile impostare con lo Scheduler Avira un job con cui aggiornare automaticamente il prodotto Avira:

- Selezionare in Control Center la rubrica **Gestione > Scheduler**.
- Fare clic sul simbolo + **Crea nuovo job con un wizard**.

  ↳ Appare la finestra di dialogo **Nome e descrizione del job**.

- Assegnare un nome al job e descriverlo.
- Fare clic su **Avanti**.

  ↳ Viene visualizzata la finestra di dialogo **Tipo di job**.

- Selezionare un **Job di aggiornamento** dalla lista.
- Fare clic su **Avanti**.

↳ Apparirà la finestra di dialogo **Durata del job**.

- Selezionare quando deve essere eseguita la scansione:

- **Immediato**
- **Giornaliero**
- **Settimanale**
- **Intervallo**
- **Unico**

> **Suggerimenti**
> Raccomandiamo di eseguire gli aggiornamenti periodicamente e con una certa frequenza. L'intervallo di aggiornamento consigliato è: 24 Ore.

- Indicare il termine in base alla selezione.
- Selezionare una delle opzioni aggiuntive (disponibili in base al tipo di job):

- **Ripeti job se il tempo è già scaduto**
  Vengono eseguiti job scaduti che non è stato possibile eseguire al momento designato, ad esempio perché il computer era spento.

- Fare clic su **Avanti**.

  ↳ Appare la finestra di dialogo **Selezione della modalità di visualizzazione**.

- Selezionare la modalità di visualizzazione della finestra del job:

- **Invisibile**: nessuna finestra del job
- **Ridotta**: solo la barra di progressione
- **Estesa**: tutta la finestra del job

- Fare clic su **Fine**.

  ↳ Il nuovo job assegnato viene visualizzato alla pagina iniziale della rubrica **Gestione > Scansiona** come attivato (segno di spunta).

- Disattivare i job che non devono essere eseguiti.

Mediante i seguenti simboli, è possibile elaborare ulteriormente i job:

Visualizza le proprietà di un job

Modifica job

Elimina job

Avvia job

Arresta job

4.3.2 Avvio di un aggiornamento manuale

Sono disponibili varie opzioni per avviare manualmente un aggiornamento: durante gli aggiornamenti avviati manualmente viene sempre eseguito anche l'aggiornamento del file di definizione dei virus e del motore di ricerca. L'aggiornamento del prodotto avviene soltanto se nella configurazione in Sicurezza del computer > Aggiornamento > Aggiornamento prodotto è stata attivata l'opzione **Scarica aggiornamenti del prodotto e installa automaticamente**.

L'aggiornamento manuale del prodotto Avira può essere avviato nel modo seguente:

- Fare clic con il tasto destro del mouse sull'icona Tray di Avira nella barra delle applicazioni e selezionare **Avvia aggiornamento**.

  \- OPPURE -

- Nel Control Center selezionare la rubrica **Panoramica > Stato**, quindi fare clic nella sezione **Ultimo aggiornamento** sul link **Avvia aggiornamento**.

  \- OPPURE -

  In Control Center, nel menu **Aggiornamento** selezionare il comando **Avvia aggiornamento**.

  ↳ Compare la finestra di dialogo **Updater**.

Suggerimenti
Raccomandiamo di eseguire gli aggiornamenti automatici periodicamente. L'intervallo di aggiornamento consigliato è: 24 Ore.

Suggerimenti
É possibile eseguire un aggiornamento anche manualmente mediante il Centro di sicurezza Windows.

4.3.3 Scansione diretta: Eseguire il controllo di virus e malware con un profilo di ricerca

Un profilo di ricerca è un insieme di drive e directory che devono essere scansionati.

Per effettuare una scansione con un profilo di ricerca è possibile:

- Utilizzare il profilo di ricerca predefinito

  Se i profili di ricerca predefiniti si adattano alle proprie esigenze.

- Modificare il profilo di ricerca e utilizzarlo (selezione manuale)

Se si desidera eseguire una scansione con un profilo di ricerca personalizzato.

In base al sistema operativo sono disponibili diversi simboli per l'avvio di un profilo di ricerca:

- In Windows XP e 2000:

  Con questo simbolo si avvia la scansione mediante un profilo di ricerca.

- In Windows Vista:

  In Microsoft Windows Vista il Control Center ha inizialmente diritti limitati ad esempio per l'accesso a file e directory. Alcune azioni e l'accesso ai file possono essere eseguiti dal Control Center solo con diritti di amministratore avanzati. Questi diritti di amministratore avanzati devono essere assegnati a ogni avvio di una scansione mediante un profilo di scansione.
  Con questo simbolo si avvia una scansione limitata mediante un profilo di ricerca. Vengono scansionati solo i file e le directory per cui Windows Vista ha concesso i diritti di accesso.
  Con questo simbolo si avvia una scansione con diritti avanzati dell'amministratore. Dopo una conferma, vengono scansionati tutti i file e le directory del profilo di ricerca selezionato.

Per cercare virus e malware con un profilo:

- Selezionare la rubrica **Sicurezza del computer > System Scanner** nel Control Center.

  ↪ Appaiono i profili di ricerca predefiniti.

- Selezionare un profilo di ricerca predefinito.

  \- OPPURE -

  Modificare il profilo di ricerca **Selezione manuale**.

- Fare clic sul simbolo (Windows XP: o Windows Vista:).
- Appare la finestra **Luke Filewalker** e si avvia la scansione diretta.

  ↪ Al termine del processo di scansione vengono visualizzati i risultati.

Se si desidera modificare un profilo di ricerca:

- Aprire nel profilo di ricerca **Selezione manuale** la struttura dei file fin quando non vengono aperti tutti i drive che devono essere scansionati:
- Selezionare i nodi che devono essere scansionati facendo clic nella casella:

4.3.4 Scansione diretta: Ricerca di virus e malware con Drag & Drop

È possibile cercare con Drag&Drop virus e malware nel modo seguente:

✓ Il Control Center del programma Avira è aperto.

- Selezionare il file, che si desidera controllare.
- Trascinare con il tasto sinistro del mouse il file selezionatonel Control Center.
  - ↳ Appare la finestra **Luke Filewalker** e si avvia la scansione diretta.
  - ↳ Al termine del processo di scansione vengono visualizzati i risultati.

4.3.5 Scansione diretta: Cerca virus e malware con il menu contestuale

Per cercare in maniera mirata virus e malware mediante il menu contestuale:

- Fare clic (ad esempio in Esplora risorse di Windows, sul desktop o in una directory aperta di Windows) con il tasto destro del mouse sul file chesi desidera controllare.
  - ↳ Appare il menu contestuale di Esplora risorse di Windows.
- Nel menu contestuale selezionare **Controlla i file selezionati con Avira**.
  - ↳ Appare la finestra **Luke Filewalker** e si avvia la scansione diretta.
  - ↳ Al termine del processo di scansione vengono visualizzati i risultati.

4.3.6 Scansione diretta: cerca automaticamente virus e malware

Suggerimenti
Una volta eseguita l'installazione il job *Scansione completa del sistema* si trova nello : in un intervallo di aggiornamento consigliato viene eseguita automaticamente una scansione completa del sistema.

Cercare automaticamente virus e malware è un job che si imposta come segue:

- Selezionare in Control Center la rubrica **Gestione > Scheduler**.
- Fare clic sul simbolo + **Crea nuovo job con un wizard**.
  - ↳ Appare la finestra di dialogo **Nome e descrizione del job**.
- Assegnare un nome al job e descriverlo.
- Fare clic su **Avanti**.
  - ↳ Appare la finestra di dialogo **Tipo di job**.
- Selezionare il **Job di scansione**.
- Fare clic su **Avanti**.
  - ↳ Appare la finestra di dialogo **Selezione del profilo**.
- Selezionare quale profilo deve essere scansionato.
- Fare clic su **Avanti**.
  - ↳ Apparirà la finestra di dialogo **Durata del job**.
- Selezionare quando deve essere eseguita la scansione:

- **Immediato**
- **Giornaliero**
- **Settimanale**
- **Intervallo**
- **Unico**

- Indicare il termine in base alla selezione.
- Selezionare una delle seguenti opzioni aggiuntive (disponibili in base al tipo di job): **Ripeti job se il tempo è già scaduto**

  ↳ Vengono eseguiti job scaduti che non è stato possibile eseguire al momento designato, ad esempio perché il computer era spento.

- Fare clic su **Avanti**.

  ↳ Appare la finestra di dialogo **Selezione della modalità di visualizzazione**.

- Selezionare la modalità di visualizzazione della finestra del job:

- **Invisibile**: nessuna finestra del job
- **Ridotta**: solo la barra di progressione
- **Estesa**: tutta la finestra del job

- Selezionare l'opzione **Spegni computer al termine del job**, se si desidera che il calcolatore si spenga automaticamente non appena il job è stato eseguito e concluso.

  L'opzione è disponibile solo nella modalità di visualizzazione ridotta o estesa.

- Fare clic su **Fine**.

  ↳ Il nuovo job assegnato viene visualizzato nella pagina iniziale della rubrica **Gestione > Scheduler** come attivato (segno di spunta).

- Disattivare i job che non devono essere eseguiti.

Mediante i seguenti simboli, è possibile elaborare ulteriormente i job:

4.3.7 Scansione diretta: Effettuare una scansione mirata per rootkit attivi

Per effettuare una ricerca di rootkit attivi, utilizzare il profilo di ricerca predefinito **Cerca rootkit e malware attivi**.

La ricerca di rootkit mirata si effettua nel modo seguente:

- Selezionare la rubrica **Sicurezza del computer > System Scanner** nel Control Center.
  - ↳ Appaiono i profili di ricerca predefiniti.
- Selezionare il profilo di ricerca predefinito **Cerca rootkit e malware attivi**.
- Evidenziare altri punti e directory che devono essere verificati con un clic nella casella del livello della directory.
- Fare clic sul simbolo (Windows XP: o Windows Vista:).
  - ↳ Appare la finestra **Luke Filewalker** e si avvia la scansione diretta.
  - ↳ Al termine del processo di scansione vengono visualizzati i risultati.

4.3.8 Reagire a virus e malware riscontrati

Per i singoli componenti di protezione del prodotto Avira in uso, è possibile impostare nella configurazione, nella rubrica **Azione in caso di rilevamento**, il modo in cui tale prodotto deve reagire al rilevamento di un virus o di un programma indesiderato.

Nel componente Realtime Protection non esiste la possibilità di configurare alcuna opzione di azione. In caso di rilevamento di un virus compare un messaggio sul desktop. È possibile rimuovere il malware rilevato direttamente nel messaggio sul desktop oppure trasmettere il malware al componente System Scanner per un ulteriore trattamento del virus selezionando il pulsante **Dettagli**. System Scanner segnala il rilevamento in una finestra, nella quale, mediante un menu contestuale, sono disponibili diverse opzioni per il trattamento del file infetto (vedere Rilevamento > System Scanner).

Opzioni di azione in System Scanner:

- **Interattivo**

  Nella modalità di azione interattiva vengono notificati i rilevamenti della scansione di System Scanner in una finestra di dialogo. Questa opzione è attivata di default.
  Al termine della scansione di System Scanner, si riceve un avviso con l'elenco dei file infetti rilevati. Mediante il menu contestuale è possibile selezionare un'azione da eseguire per i singoli file infetti. È possibile eseguire l'azione selezionata per tutti i file infetti oppure interrompere la scansione di System Scanner.

- **Automatico**

  Nella modalità di azione automatica, in caso di rilevamento di un virus o di un programma indesiderato, l'azione selezionata dall'utente in questa sezione viene eseguita automaticamente.

Opzioni di azione in Web Protection:

- **Interattivo**

  Nella modalità di azione interattiva, in caso di rilevamento di un virus o di un programma indesiderato appare una finestra di dialogo nella quale è possibile scegliere come gestire i file infetti. Questa opzione è attivata di default.

- **Automatico**

  Nella modalità di azione automatica, in caso di rilevamento di un virus o di un programma indesiderato, l'azione selezionata dall'utente in questa sezione viene eseguita automaticamente.

Modalità di azione interattiva

- Nella modalità di azione interattiva si reagisce ai virus e ai programmi indesiderati rilevati selezionando nell'avviso un'azione per gli oggetti infetti ed eseguendo l'azione selezionata mediante conferma.

Per il trattamento di oggetti infetti possono essere selezionate le seguenti azioni:

> **Suggerimenti**
> Le azioni disponibili dipendono dal sistema operativo, dal componente di protezione (Avira System Scanner, Avira Realtime Protection, Avira Web Protection) che segnala il file rilevato e dal malware rilevato.

Azioni di System Scanner:

- **Ripara**

  Il file viene riparato.
  Questa opzione è attivabile solo se è possibile riparare il file.

- **Rinomina**

  Il file viene rinominato **.vir*. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere successivamente riparati e nuovamente rinominati.

- **Quarantena**

  Il file viene compresso in un formato speciale (**.qua*) e spostato nella directory di quarantena *INFECTED* sull'hard disk, in modo da escludere qualsiasi accesso diretto. I file in questa directory possono essere successivamente riparati nella quarantena o, se necessario, inviati ad Avira.

- **Elimina**

  Il file viene eliminato.
  Se il file rilevato è un virus del record di avvio eliminarlo con Elimina. Viene scritto un nuovo record di avvio.

- **Ignora**

  Non viene eseguita alcuna altra azione. Il file infetto rimane attivo sul computer.

> **Attenzione**
> Pericolo di perdita di dati e danni al sistema operativo!
> Utilizzare l'opzione **Ignora** solo in casi eccezionali e fondati.

- **Ignora sempre**

  Opzione di azione in caso di file rilevati da Realtime Protection: Realtime Protection non esegue alcuna altra azione. L'accesso al file viene autorizzato. Vengono autorizzati tutti gli accessi successivi a questo file e non si ricevono comunicazioni fino al riavvio del computer o a un aggiornamento del file di definizione dei virus.

- **Copia in quarantena**

  Opzione di azione in caso di rilevamento di un Rootkits: il file rilevato viene copiato nella quarantena.

- **Ripara record di avvio | Scarica strumento di riparazione**

  Opzioni di azione in caso di rilevamento di record di avvio infetto: in caso di drive del floppy disk infetti sono disponibili opzioni per effettuare la riparazione. Se con il prodotto Avira non è possibile effettuare alcuna riparazione, è possibile scaricare uno strumento speciale che riconosce e rimuove i virus del record di avvio.

> **Suggerimenti**
> Se si applicano azioni su processi in corso, i processi interessati vengono terminati prima dell'esecuzione dell'azione.

Azioni di Web Protection:

- **Nega accesso**

  Il sito Web richiesto dal server Web o i dati e i file trasferiti non vengono inviati al proprio browser Web. Nel browser Web viene visualizzato un messaggio di errore relativo al divieto di accesso.

- **Quarantena**

  Il sito web richiesto dal server web o i dati e i file trasferiti non vengono spostati nella quarantena. Il file infetto può essere ripristinato dal Gestore della quarantena se ha un valore informativo, oppure, se necessario, inviato ad Avira Malware Research Center.

- **Ignora**

  Il sito Web richiesto dal server Web o i dati e i file trasferiti vengono inoltrati da Web Protection al proprio browser Web.

Attenzione
In questo modo virus e programmi indesiderati potrebbero accedere al computer. Selezionare l'opzione **Ignora** solo in casi eccezionali.

Suggerimenti
Consigliamo di spostare in quarantena un file sospetto che non può essere riparato.

4.3.9 Quarantena: Trattare file (*.qua) in quarantena

É possibile trattare i file in quarantena nel modo seguente:

- Selezionare la rubrica **Gestione > Quarantena** nel Control Center.
- Verificare di quali file si tratta cosicché sia possibile ripristinare gli originali sul computer.

Se si desidera visualizzare maggiori informazioni su un file:

- Selezionare il file e fare clic su i.
  - ↳ Apparirà la finestra di dialogo **Proprietà** con ulteriori informazioni sul file.

Se si desidera verificare nuovamente un file:

La verifica di un file è consigliata quando il file di definizione dei virus del prodotto Avira è stato aggiornato ed esiste il sospetto di un falso allarme. É così possibile confermare un falso allarme a una successiva verifica e ripristinare il file.

- Selezionare il file e fare clic su .
  - ↳ Il file viene controllato utilizzando le impostazioni della scansione diretta per virus e malware.
  - ↳ Dopo il controllo appare la finestra di dialogo **Statistiche della scansione** che visualizza la statistica relativa allo stato del file prima e dopo la nuova scansione.

Se si desidera eliminare un file:

- Selezionare il file e fare clic su ×.
- Occorre confermare la selezione effettuata mediante **Sì**.

Se si desidera caricare il file da analizzare su un server Web di Avira Malware Research Center:

- Selezionare il file che si desidera caricare.

- Fare clic su .
  - ↳ Si aprirà la finestra di dialogo *Carica file* con un modulo per inserire i dati personali a cui essere contattati.
- Indicare per intero i propri dati.
- Selezionare un tipo: **File sospetto** oppure **Sospetto di Falso allarme**.
- Selezionare un formato di risposta: **HTML**, **Testo**, **HTML & Testo**.
- Fare clic su **OK**.
  - ↳ Il file compresso viene caricato su un server Web di Avira Malware Research Center.

Suggerimenti
Nei seguenti casi si consiglia un'analisi da parte di Avira Malware Research Center:
Oggetto euristico (file sospetto): durante una scansione, un file del prodotto Avira è stato identificato come sospetto e spostato in quarantena: Nella finestra di dialogo per il rilevamento di virus o nel file di report della scansione è stata consigliata l'analisi del file da parte di Avira Malware Research Center.
Sospetto di

Suggerimenti
La dimensione dei file caricati si limita a 20 MB non compressi o a 8 MB compressi.

Suggerimenti
È possibile caricare solo un singolo file.

Se si desidera esportare in un file di testo le proprietà di un oggetto in quarantena selezionato:

- Selezionare il file in quarantena e fare clic su .
  - ↳ Si apre il file di testo *Quarantena - Editor* con i dati dell'oggetto in quarantena scelto.
- Salvare il file di testo.

I file in quarantena possono anche essere ripristinati (vedere Capitolo: Quarantena: Ripristina file in quarantena

4.3.10 Quarantena: Ripristina file in quarantena

In base al sistema operativo sono disponibili diversi sistemi per il ripristino:

- **In Windows XP e 2000**:

  Con questo simbolo si ripristinano i file nella directory originale.

  Con questo simbolo si ripristinano i file nella directory selezionata.

- **In Windows Vista**:

  In Microsoft Windows Vista il Control Center ha inizialmente diritti limitati ad esempio per l'accesso a file e directory. Alcune azioni e l'accesso ai file possono essere eseguiti dal Control Center solo con diritti di amministratore avanzati. Questi diritti di amministratore avanzati devono essere assegnati a ogni avvio di una scansione mediante un profilo di scansione.

  Con questo simbolo si ripristinano i file nella directory selezionata.

  Con questo simbolo si ripristinano i file nella directory originale. Se per l'accesso a questa directory sono necessari diritti di amministratore avanzati, appare una richiesta corrispondente.

É possibile ripristinare i file in quarantena nel modo seguente:

> **Attenzione**
> Pericolo di perdita di dati e danni al sistema operativo del computer! Utilizzare la funzione **Ripristina l'oggetto selezionato** solo in casi eccezionali. Ripristinare solo quei file che possono essere riparati con una nuova scansione.

✓ File nuovamente controllato e riparato con una scansione.

▶ Selezionare la rubrica **Gestione > Quarantena** nel Control Center.

> **Suggerimenti**
>
> Le email e gli allegati possono essere ripristinati solo con l'opzione e con l'estensione **.eml*.

Se si desidera ripristinare un file nella sua posizione originale:

▶ Evidenziare il file e fare clic sul simbolo (Windows 2000/XP: , Windows Vista).

Questa opzione non è disponibile per le email.

Suggerimenti

Le email e gli allegati possono essere ripristinati solo con l'opzione e con l'estensione **.eml*.

↳ Viene richiesto quindi se si desidera ripristinare il file.

- Fare clic su **Sì**.

  ↳ Il file viene ripristinato nella directory dalla quale è stato spostato in quarantena.

Se si desidera ripristinare un file in una determinata directory:

- Selezionare il file e fare clic su .

  ↳ Viene richiesto quindi se si desidera ripristinare il file.
- Fare clic su **Sì**.

  ↳ Apparirà la finestra standard di Windows per la selezione di una directory.
- Selezionare la directory nella quale si desidera ripristinare il file e confermare.

  ↳ Il file viene ripristinato nella directory selezionata.

4.3.11 Quarantena: Sposta i file sospetti in quarantena

É possibile spostare in quarantena i file sospetti manualmente come segue:

- Selezionare la rubrica **Gestione > Quarantena** nel Control Center.
- Fare clic su +.

  ↳ Apparirà la finestra standard di Windows per la selezione di un file.
- Selezionare il file e confermare con **Apri**.

  ↳ Il file viene spostato in quarantena.

È possibile controllare i file in quarantena con Avira System Scanner (vedere Capitolo: Quarantena: Trattare file (*.qua) in quarantena).

4.3.12 Profilo di ricerca: Inserisci o elimina un tipo di file in un profilo di ricerca

Per stabilire per un profilo di ricerca i tipi di file da scansionare o i tipi di file che devono essere esclusi dalla ricerca (possibile solo con selezione manuale):

✓ In Control Center, nella rubrica **Sicurezza del computer > Verifica**.

- fare clic con il tasto destro del mouse sul profilo di ricerca che si desidera modificare.

  ↳ Apparirà un menu contestuale.
- Selezionare la voce **Filtro file**.

- Aprire nuovamente il menu contestuale facendo clic sul piccolo triangolo sul lato destro del menu contestuale.
  - ↳ Appariranno le voci **Standard**, **Controlla tutti i file** e **Personalizzato**.
- Selezionare la voce **Personalizzato**.
  - ↳ Apparirà la finestra di dialogo **Estensione file** con un elenco di tutti i tipi di file che devono essere abbinati al profilo di ricerca.

Se si desidera escludere un tipo di file dalla scansione:

- Selezionare il tipo di file e fare clic su **Elimina**.

Se si desidera aggiungere un tipo di file dalla scansione:

- Selezionare un tipo di file.
- Fare clic su **Aggiungi** e inserire l'estensione del tipo di file nel campo.

  Utilizzare un massimo di 10 caratteri e non inserire punti. Le wildcard (* e ?) sono consentite.

4.3.13 Profilo di ricerca: Creare un collegamento sul desktop per il profilo di ricerca

Mediante un collegamento sul desktop per un profilo di ricerca è possibile avviare una scansione diretta facendo clic sul desktop senza richiamare il Control Center del prodotto Avira.

É possibile creare un collegamento al profilo di ricerca dal desktop:

- ✓ In Control Center, nella rubrica **Sicurezza del computer > Verifica**.
- selezionare il profilo di ricerca di cui si intende creare il collegamento.
- Fare clic sul simbolo .
  - ↳ Viene creato un collegamento sul desktop.

4.3.14 Eventi: Filtrare eventi

Nel Control Center, in **Gestione > Eventi**, vengono visualizzati eventi creati dai componenti del prodotto Avira (analogamente al visualizzatore eventi del sistema operativo di Windows). Di seguito sono riportati i componenti del programma:

- Web Protection
- Realtime Protection
- Servizio di assistenza
- Scheduler
- System Scanner

- Updater

Vengono visualizzati i seguenti tipi di eventi:

- *Informazioni*
- *Attenzione*
- *Errore*
- *Rilevamento*

Come filtrare gli eventi visualizzati:

- Selezionare nel Control Center la rubrica **Gestione > Eventi**.
- Attivare la casella delle componenti di programma per visualizzare gli eventi delle componenti attive.

  - OPPURE -

  Disattivare la casella di spunta dei componenti di programma per non visualizzare gli eventi dei componenti disattivati.
- Attivare la casella dei tipi di evento per visualizzare questi eventi.

  - OPPURE -

  Disattivare la casella di spunta dei tipi di evento per non visualizzare questi eventi.

5. System Scanner

Con il componente System Scanner è possibile effettuare scansioni mirate per virus e programmi indesiderati (scansione diretta). È possibile effettuare una scansione per file infetti in diversi modi:

- **Scansione diretta mediante menu contestuale**
  La scansione diretta mediante il menu contestuale (tasto destro del mouse - voce **Controlla i file selezionati con Avira**) si consiglia quando, ad esempio, si desidera controllare singoli file e directory in Esplora risorse di Windows. Un ulteriore vantaggio è che il Control Center non deve essere avviato per la scansione diretta mediante il menu contestuale.
- **Scansione diretta con Drag & Drop**
  Trascinando un file o una directory nella finestra di programma del Control Center System Scanner verifica il file o la directory, nonché tutte le sottodirectory. Questa procedura è consigliata quando si desidera controllare i singoli file e directory che sono stati archiviati, ad esempio, sul desktop.
- **Scansione diretta per profili**
  Questa procedura è consigliata quando si desidera controllare regolarmente alcune directory e drive (ad esempio la propria directory di lavoro o drive, sui quali si archiviano regolarmente nuovi file). Queste directory e drive non devono quindi essere selezionati a ogni scansione ma vengono comodamente selezionati tramite il profilo corrispondente. Vedere Scansione diretta per profili.
- **Scansione diretta con Scheduler**
  offre la possibilità di far eseguire job temporizzati di scansione. Vedere Scansione diretta con Scheduler.

Durante la scansione per rootkit, virus del record di avvio e durante la scansione dei processi attivi sono necessari dei procedimenti particolari. Sono disponibili le seguenti opzioni:

- Cerca rootkit mediante il profilo di ricerca *Cerca rootkit e malware attivi*
- Scansione dei processi attivi mediante il profilo di ricerca *Processi attivi*
- Scansiona virus del record di avvio con il comando **Scansiona virus del record di avvio...** nel menu **Extra**

6. Aggiornamenti

L'efficacia di un software antivirus dipende dall'aggiornamento del programma, in particolare del file di definizione dei virus e del motore di ricerca. Per l'esecuzione degli aggiornamenti, il componente Updater è integrato nel prodotto Avira. Updater garantisce che il prodotto Avira sia sempre il più aggiornato possibile e che sia in grado di rilevare i nuovi virus che compaiono quotidianamente. Updater aggiorna i seguenti componenti:

- File di definizione dei virus:

  Il file di definizione dei virus contiene il modello di rilevamento del programma dannoso che il prodotto Avira utilizza nella scansione per virus e malware nonché nella riparazione di oggetti infetti.

- Motore di ricerca:

  Il motore di ricerca contiene i metodi che vengono utilizzati dal prodotto Avira per la scansione per virus e malware.

- File di programma (aggiornamento del prodotto):

  I pacchetti di aggiornamento del prodotto mettono a disposizione ulteriori funzioni per i singoli componenti del programma.

Durante un aggiornamento viene verificato lo stato di aggiornamento del file di definizione dei virus e del motore di ricerca e, se necessario, tali componenti vengono aggiornati. In base alle impostazioni di configurazione Updater esegue un aggiornamento del prodotto o segnala la disponibilità di tale aggiornamento. Terminato un aggiornamento del prodotto può essere necessario riavviare il sistema. Se l'aggiornamento avviene solo per il file di definizione dei virus e del motore di ricerca non è necessario riavviare il computer.

> **Suggerimenti**
> Per motivi di sicurezza, l'Updater verifica se il file host di Windows del computer è stato modificato, ad esempio con manipolazione da parte di malware dell'URL di aggiornamento, a seguito della quale l'Updater viene indirizzato su pagine di download indesiderate. Se il file host di Windows è stato manipolato, l'evento viene riportato nel file di report di Updater.

Un aggiornamento viene eseguito in automatico nel seguente intervallo: 24 Ore. È possibile modificare o disattivare l'aggiornamento automatico dalla configurazione (Configurazione > Aggiorna).

Nel Control Center sotto **Scheduler** è possibile configurare ulteriori job di aggiornamento che Updater deve eseguire a intervalli definiti. È inoltre possibile avviare l'aggiornamento manualmente:

- In Control Center: nel menu **Aggiornamento** e nella rubrica **Stato**
- Tramite il menu contestuale dell'icona Tray

Gli aggiornamenti vengono richiamati da Internet tramite un server Web del produttore. Normalmente si utilizza la connessione di rete esistente per collegarsi al server di download di Avira. Questa impostazione standard può essere modificata nella configurazione in Generale > Aggiorna.

7. Risoluzione di problemi, suggerimenti

7.1 Panoramica

In questo capitolo sono presenti indicazioni importanti per la risoluzione di problemi e ulteriori suggerimenti inerenti al prodotto Avira acquistato.

- Vedere capitolo Assistenza in caso di problemi
- Vedere capitolo Shortcut
- Vedere capitolo Centro di sicurezza di Windows

7.2 Assistenza in caso di problemi

Qui sono reperibili informazioni sulle cause e le soluzioni di eventuali problemi.

- Nel tentativo di avviare un aggiornamento apre un messaggio di errore *Lo stabilimento della connessione è fallito durante il download del file ....*
- Impossibile spostare o eliminare virus e malware.
- L'icona Tray mostra uno stato disattivato.
- Il computer è estremamente lento se effettuo il salvataggio di dati.
- Il mio Firewall segnala i servizi Avira Realtime Protection, se è attivo.
- Webchat non funziona: non vengono visualizzati i messaggi chat.

Il messaggio di errore *Lo stabilimento della connessione è fallito durante il download del file ...* appare nel tentativo di avviare un aggiornamento.

Causa: la connessione Internet non è attiva. Pertanto, non può essere creato alcun collegamento al server Web in Internet.

- Provare se altri servizi Internet come WWW o l'email funzionano. Se non funzionano ripristinare la connessione Internet.

Causa: il server proxy non è raggiungibile.

- Verificare se sia cambiato il login per il server proxy e adattare eventualmente la propria configurazione.

Causa: il file update.exe non è ammesso dal proprio firewall.

- Assicurarsi che il file update.exe sia ammesso dal proprio firewall.

Altrimenti:

- Controllare le impostazioni nella configurazione (modalità esperto) in Generale > Aggiornamento.

Impossibile spostare o eliminare virus e malware.

Causa: il file è stato caricato da Windows ed è attivo.

- Aggiornare il prodotto Avira acquistato.
- Se si utilizza il sistema operativo Windows XP, disattivare il ripristino del sistema.
- Avviare il computer in modalità provvisoria.
- Avviare il programma Avira e la configurazione (Modalità esperto).
- Selezionare **System Scanner > Scansione > File > Tutti i file** e confermare la finestra con **OK**.
- Avviare una scansione su tutti i drive locali.
- Avviare il computer in modalità normale.
- Eseguire una scansione in modalità normale.
- Se non vengono rilevati altri virus e malware attivare il ripristino del sistema se è disponibile e deve essere utilizzato.

L'icona Tray mostra uno stato disattivato.

Causa: Il servizio Avira Realtime Protection è disattivato.

- Nel Control Center fare clic nella rubrica **Panoramica > Stato** nella sezione **Avira Realtime Protection** sul link **Attiva**.

Causa: Avira Realtime Protection è bloccato da un firewall.

- Nella configurazione del firewall definire un permesso generale per Avira Realtime Protection. Avira Realtime Protection lavora esclusivamente con l'indirizzo 127.0.0.1 (localhost). Non viene stabilita alcuna connessione internet.

Altrimenti:

- Verificare la modalità di attivazione del servizio Avira Realtime Protection. Attiva eventualmente il servizio: selezionare in **Start > Impostazioni > Pannello di controllo**. Avviare il pannello di configurazione **Servizi** facendo doppio clic (in Windows 2000 e Windows XP l'applet servizi si trova nella sottodirectory *Gestione*). Cercare la voce *Avira Realtime Protection*. Come modalità di avviamento deve essere inserito `Automatico` e come stato `Avviato`. Avviare il servizio manualmente mediante la selezione della riga corrispondente e del pulsante **Avvia**. Se viene visualizzato un messaggio di errore, verificare la visualizzazione eventi.

Il computer diventa estremamente lento se eseguo un backup.

Causa: Avira Realtime Protection scansiona tutti i dati con i quali lavora il backup durante il processo di backup.

- Selezionare nella configurazione (modalità esperto) **Realtime Protection > Scansione > Eccezioni** e inserire il nome del processo del software di backup.

Il mio Firewall segnala i servizi Avira Realtime Protection, se è attivo.

Causa: La comunicazione di Avira Realtime Protection avviene mediante il protocollo Internet TCP/IP. Un firewall monitora tutte le connessioni mediante questo protocollo.

- Nella configurazione del firewall definire un permesso generale per Avira Realtime Protection. Avira Realtime Protection lavora esclusivamente con l'indirizzo 127.0.0.1 (localhost). Non viene stabilita alcuna connessione internet.

> **Suggerimenti**
> Consigliamo di eseguire regolarmente gli aggiornamenti Microsoft per colmare le eventuali lacune in termini di sicurezza.

Webchat non funziona: i messaggi chat non vengono visualizzati, nel browser vengono caricati dei dati.

Questo fenomeno può verificarsi in chat che si basano sul protocollo HTTP con 'transfer-encoding=chunked'.

Causa: Web Protection controlla i dati inviati in modo completo alla ricerca di virus e programmi indesiderati prima che i dati siano caricati nel browser Web. Durante un trasferimento di dati con 'transfer-encoding=chunked' Web Protection non è in grado di rilevare la lunghezza dei messaggi o la quantità di dati.

- Nella configurazione impostare l'URL di Webchat come eccezione (vedere Configurazione: Web Protection > Eccezioni).

7.3 Shortcut

Le shortcut offrono la possibilità di navigare velocemente nel programma, richiamare singoli moduli e avviare azioni.

Di seguito viene presentata una panoramica delle shortcut presenti. Per maggiori informazioni sulla funzionalità e disponibilità consultare il capitolo corrispondente della guida.

7.3.1 Nelle finestre di dialogo

Shortcut	Descrizione
Ctrl + Tab **Ctrl + Page down**	Navigazione in Control Center Passa alla rubrica successiva.
Ctrl + Shift + Tab **Ctrl + Page down**	Navigazione in Control Center Passa alla rubrica precedente.
← ↑ → ↓	Navigazione nelle rubriche di configurazione Evidenzia con il mouse una rubrica di configurazione.
Tab	Passa all'opzione successiva o al successivo gruppo di opzioni.
Shift + Tab	Passa all'opzione precedente o al precedente gruppo di opzioni.
← ↑ → ↓	Effettua una modifica tra le opzioni di un menu a tendina selezionate o tra più opzioni in un gruppo di opzioni.
Barra spaziatrice	Attiva o disattiva una casella di controllo se l'opzione attiva è una casella di controllo.
Alt + lettera sottolineata	Seleziona l'opzione o esegui il comando.
Alt + ↓ **F4**	Apri il menu a tendina selezionato.
Esc	Chiudi il menu a tendina selezionato. Annulla il comando e chiudi la finestra di dialogo.

Invio	Esegui comando per l'opzione o il pulsante attivo.

7.3.2 Nella Guida in linea

Shortcut	Descrizione
Alt + barra spaziatrice	Visualizza il menu del sistema.
Alt + Tab	Passa dalla Guida in linea ad altre finestre aperte.
Alt + F4	Chiudi la Guida in linea.
Shift+ F10	Visualizza menu contestuali della Guida in linea.
Ctrl + Tab	Passa alla rubrica successiva nella finestra di navigazione.
Ctrl + Shift + Tab	Passa alla rubrica precedente nella finestra di navigazione.
Page up	Passa all'argomento che è visualizzato sopra l'argomento attuale nel sommario, nell'indice o nell'elenco dei risultati della ricerca.
Page down	Passa all'argomento che è visualizzato sotto l'argomento attuale nel sommario, nell'indice o nell'elenco dei risultati della ricerca.
Page up **Page down**	Sfoglia le voci su un argomento.

7.3.3 In Control Center

Generale

Shortcut	Descrizione
F1	Visualizza Guida in linea
Alt + F4	Chiudi Control Center

F5	Aggiorna visualizzazione
F8	Apri configurazione
F9	Avvia aggiornamento

Rubrica **Scansiona**

Shortcut	Descrizione
F3	Avvia la scansione con il profilo selezionato
F4	Crea collegamento sul desktop per il profilo selezionato

Rubrica **Quarantena**

Shortcut	Descrizione
F2	Riscansiona l'oggetto
F3	Ripristina l'oggetto
F4	Invia l'oggetto
F6	Ripristina l'oggetto in...
Invio	Proprietà
Agg	Aggiungi file
Canc	Elimina l'oggetto

Rubrica **Scheduler**

Shortcut	Descrizione
F2	Modifica job
Invio	Proprietà
Agg	Inserisci nuovo job
Canc	Elimina job

Rubrica **Report**

Shortcut	Descrizione
F3	Visualizza il file di report
F4	Stampa il file di report
Invio	Mostra il report
Canc	Elimina il report

Rubrica **Eventi**

Shortcut	Descrizione
F3	Esporta evento
Invio	Mostra evento
Canc	Elimina evento

7.4 Centro di sicurezza di Windows

- a partire da Windows XP Service Pack 2 -

7.4.1 Generale

Il Centro sicurezza di Windows verifica lo stato di un computer dal punto di vista della sicurezza.

Se viene rilevato un problema in uno di questi punti importanti (ad esempio un programma antivirus vecchio), il Centro sicurezza invia un avviso e fornisce dei suggerimenti per proteggere più efficacemente il computer.

7.4.2 Il Centro sicurezza di Windows e il prodotto Avira acquistato

Software di protezione antivirus/Protezione da software dannoso

È possibile ricevere i seguenti avvisi dal Centro sicurezza di Windows in relazione alla protezione antivirus.

- Protezione antivirus NON TROVATA
- Protezione antivirus NON AGGIORNATA
- Protezione antivirus ATTIVA
- Protezione antivirus INATTIVA
- Protezione antivirus NON MONITORATA

Protezione antivirus NON TROVATA

Questo avviso del Centro sicurezza di Windows viene visualizzato quando quest'ultimo non ha rilevato alcun software antivirus sul computer.

« Tutti gli elementi del Pannello di controllo ▸ Centro operativo

Cerca nel Pannello di controllo

Pagina iniziale Pannello di controllo

Modifica impostazioni Centro operativo

Modifica impostazioni di Controllo dell'account utente

Visualizza messaggi archiviati

Visualizza informazioni sulle prestazioni

Vedere anche

Backup e ripristino

Windows Update

Risoluzione problemi di compatibilità di Windows

Rivedi i messaggi recenti e risolvi i problemi

Centro operativo: sono stati rilevati uno o più problemi.

Sicurezza

Spyware e protezione da software indesiderato (Importante)

Windows Defender è disattivato.

Attiva ora

Disattiva i messaggi relativi a: protezione da spyware e da programmi correlati

Recuperare un altro programma antispyware online

Protezione da virus (Importante)

Impossibile trovare software antivirus installato nel computer.

Trova programma online

Disattiva i messaggi relativi a: protezione da virus

Firewall di rete (Importante)

Windows Firewall è disattivato o configurato in modo errato.

Attiva ora

Disattiva i messaggi relativi a: firewall di rete

Recuperare un altro programma firewall online

Windows Update

Windows Update è impostato per chiedere conferma prima di scaricare e installare gli aggiornamenti.

Cambia impostazioni...

Disattiva i messaggi relativi a: Windows Update

Manutenzione

Imposta backup

Il backup dei file non è in corso.

Imposta backup

Disattiva i messaggi relativi a: Windows Backup

Suggerimenti

Installare il prodotto Avira sul computer per proteggerlo da virus e altri programmi indesiderati!

Protezione antivirus NON AGGIORNATA

Se si possiede Windows XP Service Pack 2 o Windows Vista e si installa successivamente il prodotto Avira oppure si installa Windows XP Service Pack 2 o Windows Vista su un sistema su cui è già installato il prodotto Avira, si riceve il seguente messaggio:

Pannello di controllo ▸ Sistema e sicurezza ▸ Centro operativo

Cerca nel Pannello di controllo

Pagina iniziale Pannello di controllo

Modifica impostazioni Centro operativo

Modifica impostazioni di Controllo dell'account utente

Visualizza messaggi archiviati

Visualizza informazioni sulle prestazioni

Vedere anche

Backup e ripristino

Windows Update

Risoluzione problemi di compatibilità di Windows

Rivedi i messaggi recenti e risolvi i problemi

Centro operativo: sono stati rilevati uno o più problemi.

Sicurezza

Spyware e protezione da software indesiderato (Importante)

Avira Desktop non è aggiornato.

Aggiorna

Disattiva i messaggi relativi a: protezione da spyware e da programmi correlati

Recuperare un altro programma antispyware online

Protezione da virus (Importante)

Avira Desktop non è aggiornato.

Aggiorna ora

Disattiva i messaggi relativi a: protezione da virus

Recuperare un altro programma antivirus online

Windows Update

Windows Update è impostato per chiedere conferma prima di scaricare e installare gli aggiornamenti.

Cambia impostazioni...

Disattiva i messaggi relativi a: Windows Update

Manutenzione

Imposta backup

Il backup dei file non è in corso.

Imposta backup

Disattiva i messaggi relativi a: Windows Backup

Se l'elenco non contiene il problema in questione, provare uno dei metodi seguenti:

Risoluzione dei problemi
Trova e risolve i problemi

Ripristino
Ripristina una condizione precedente del computer

Suggerimenti

Per far sì che il Centro sicurezza di Windows riconosca il prodotto Avira come aggiornato, dopo l'installazione è necessario eseguire un aggiornamento. Aggiornare il sistema eseguendo un aggiornamento.

Protezione antivirus ATTIVA

Dopo l'installazione del prodotto Avira e un susseguente aggiornamento, si riceve la seguente nota:

Pannello di controllo ▸ Sistema e sicurezza ▸ Centro operativo
Cerca nel Pannello di controllo

Pagina iniziale Pannello di controllo
Modifica impostazioni Centro operativo
Modifica impostazioni di Controllo dell'account utente
Visualizza messaggi archiviati
Visualizza informazioni sulle prestazioni

Rivedi i messaggi recenti e risolvi i problemi
Centro operativo: sono stati rilevati uno o più problemi.

Sicurezza

Spyware e protezione da software indesiderato (Importante)
Avira Desktop non è aggiornato.
Aggiorna
Disattiva i messaggi relativi a: protezione da spyware e da programmi correlati
Recuperare un altro programma antispyware online

Protezione da virus (Importante)
Avira Desktop non è aggiornato.
Aggiorna ora
Disattiva i messaggi relativi a: protezione da virus
Recuperare un altro programma antivirus online

Windows Update
Windows Update è impostato per chiedere conferma prima di scaricare e installare gli aggiornamenti.
Cambia impostazioni...
Disattiva i messaggi relativi a: Windows Update

Manutenzione

Imposta backup
Il backup dei file non è in corso.
Imposta backup
Disattiva i messaggi relativi a: Windows Backup

Se l'elenco non contiene il problema in questione, provare uno dei metodi seguenti:

Risoluzione dei problemi
Trova e risolve i problemi

Ripristino
Ripristina una condizione precedente del computer

Vedere anche
Backup e ripristino
Windows Update
Risoluzione problemi di compatibilità di Windows

Il prodotto Avira è aggiornato e Avira Realtime Protection è attivo.

Protezione antivirus INATTIVA

Si riceve la seguente nota se si disattiva Avira Realtime Protection o si arresta il servizio.

Pannello di controllo ▸ Sistema e sicurezza ▸ Centro operativo
Cerca nel Pannello di controllo

Pagina iniziale Pannello di controllo
Modifica impostazioni Centro operativo
Modifica impostazioni di Controllo dell'account utente
Visualizza messaggi archiviati
Visualizza informazioni sulle prestazioni

Rivedi i messaggi recenti e risolvi i problemi
Centro operativo: sono stati rilevati uno o più problemi.

Sicurezza

Spyware e protezione da software indesiderato (Importante)
Avira Desktop non è aggiornato.
Aggiorna
Disattiva i messaggi relativi a: protezione da spyware e da programmi correlati
Recuperare un altro programma antispyware online

Protezione da virus (Importante)
Avira Desktop non è aggiornato.
Aggiorna ora
Disattiva i messaggi relativi a: protezione da virus
Recuperare un altro programma antivirus online

Windows Update
Windows Update è impostato per chiedere conferma prima di scaricare e installare gli aggiornamenti.
Cambia impostazioni...
Disattiva i messaggi relativi a: Windows Update

Manutenzione

Imposta backup
Il backup dei file non è in corso.
Imposta backup
Disattiva i messaggi relativi a: Windows Backup

Vedere anche
Backup e ripristino
Windows Update
Risoluzione problemi di compatibilità di Windows

Se l'elenco non contiene il problema in questione, provare uno dei metodi seguenti:
Risoluzione dei problemi
Trova e risolve i problemi
Ripristino
Ripristina una condizione precedente del computer

> **Suggerimenti**
> È possibile attivare e disattivare Avira Realtime Protection nella rubrica Panoramica > Stato del Control Center. Inoltre Avira Realtime Scanner viene riconosciuto come attivato quando l'ombrellino rosso nella barra delle applicazioni è aperto.

Protezione antivirus NON MONITORATA

Si riceve il seguente messaggio dal Centro sicurezza di Windows poiché si è optato per l'automonitoraggio del software antivirus.

> **Suggerimenti**
> La funzione non è supportata da Windows Vista.

Pannello di controllo ▸ Sistema e sicurezza ▸ Centro operativo

Cerca nel Pannello di controllo

Pagina iniziale Pannello di controllo

Modifica impostazioni Centro operativo

Modifica impostazioni di Controllo dell'account utente

Visualizza messaggi archiviati

Visualizza informazioni sulle prestazioni

Vedere anche

Backup e ripristino

Windows Update

Risoluzione problemi di compatibilità di Windows

Rivedi i messaggi recenti e risolvi i problemi

Centro operativo: sono stati rilevati uno o più problemi.

Sicurezza

Spyware e protezione da software indesiderato (Importante)

Avira Desktop non è aggiornato.

Aggiorna

Disattiva i messaggi relativi a: protezione da spyware e da programmi correlati

Recuperare un altro programma antispyware online

Protezione da virus (Importante)

Avira Desktop non è aggiornato.

Aggiorna ora

Disattiva i messaggi relativi a: protezione da virus

Recuperare un altro programma antivirus online

Windows Update

Windows Update è impostato per chiedere conferma prima di scaricare e installare gli aggiornamenti.

Cambia impostazioni...

Disattiva i messaggi relativi a: Windows Update

Manutenzione

Imposta backup

Il backup dei file non è in corso.

Imposta backup

Disattiva i messaggi relativi a: Windows Backup

Se l'elenco non contiene il problema in questione, provare uno dei metodi seguenti:

Risoluzione dei problemi
Trova e risolve i problemi

Ripristino
Ripristina una condizione precedente del computer

Suggerimenti

Il Centro sicurezza di Windows è supportato dal prodotto Avira acquistato. È possibile attivare questa opzione in ogni momento con il pulsante **Consigli...**.

Suggerimenti

Anche se sono installati Windows XP Service Pack 2 o Windows Vista, si ha comunque bisogno di una soluzione antivirus. Sebbene Windows XP Service Pack 2 controlli il software antivirus non ha alcuna funzione antivirus. L'utente non sarebbe protetto contro virus e malware senza una soluzione antivirus aggiuntiva!

8. Virus e altro

8.1 Categorie di minacce

Adware

Con Adware si designa un software che mostra all'utente i banner e i pop up pubblicitari. Questi inserti pubblicitari generalmente non possono essere chiusi e sono quasi sempre visibili. I dati della connessione permettono numerosi feedback sul comportamento dell'utente e sono problematici per motivi di sicurezza dei dati.

Il prodotto Avira riconosce Adware. Se nella configurazione in Categorie delle minacce l'opzione **Adware** è attivata, si riceve un avviso quando il prodotto Avira rileva tale software.

Adware/Spyware

Software che visualizza messaggi pubblicitari o che invia i dati personali dell'utente, spesso a sua insaputa, a terzi e che risulta quindi indesiderato.

Il prodotto Avira riconosce "Adware/Spyware". Se nella configurazione in Categorie delle minacce l'opzione **Adware/Spyware** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira effettua un rilevamento.

Applicazione

Con la denominazione "Applicazione" si intende un'applicazione il cui utilizzo può essere rischioso o la cui origine è dubbia.
Il prodotto Avira riconosce l'"Applicazione" (APPL). Se nella configurazione in Categorie delle minacce l'opzione **Applicazione** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira rileva un tale comportamento.

Software di gestione Backdoor

Per prelevare dati o manipolare il sistema viene inserito "dalla porta posteriore" un programma server backdoor senza che l'utente se ne accorga. Questo programma può essere gestito da terzi mediante Internet o la rete con un software di gestione backdoor (Client).
Il prodotto Avira riconosce il "Software di gestione Backdoor". Se nella configurazione in Categorie delle minacce l'opzione **Software di gestione Backdoor** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira effettua un rilevamento.

File con estensioni nascoste

File eseguibili che occultano la propria estensione in modo sospetto. Il metodo dell'occultamento viene spesso utilizzato dai malware.

Il prodotto Avira riconosce i "file con estensioni nascoste". Se nella configurazione in Categorie delle minacce l'opzione **File con estensioni nascoste** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira effettua un rilevamento.

Programma di selezione a pagamento

Alcuni servizi offerti in Internet sono a pagamento. In Germania la fatturazione avviene per programmi di selezione con i numeri 0190/0900 (in Austria e Svizzera con i numeri 09x0; in Germania a medio termine passerà ai numeri 09x0). Installati sul computer, questi programmi - in breve dialer - garantiscono la creazione della connessione mediante i numeri Premium-Rate, la cui tariffa può variare enormemente.

La commercializzazione di contenuti online mediante la bolletta telefonica è legale e può essere vantaggiosa per l'utente. I dialer seri non hanno alcun dubbio sul fatto che il cliente sia consapevole e lo utilizzi in modo avveduto. Tali contenuti si installano sul computer dell'utente solo se l'utente dà la propria approvazione, espressa sulla base di un'etichettatura ben riconoscibile o di una richiesta univoca e chiara. La creazione della connessione di programmi dialer seri viene visualizzata in maniera chiara e non ambigua. Inoltre, i dialer seri informano l'utente in maniera esatta e precisa sui costi correlati.

Purtroppo però esistono dialer che si installano senza farsi notare, in maniera dubbia o addirittura fraudolenta. Sostituiscono, ad esempio, la connessione standard dial up dell'utente di Internet all'ISP (Internet-Service-Provider) e a ogni connessione selezionano numeri a pagamento spesso estremamente costosi, come i numeri 0190/0900. L'utente interessato nota dalla bolletta successiva che si è installato un programma dialer indesiderato che si connette a ogni accesso a Internet ai numeri a pagamento 0190/0900 - determinando così una bolletta estremamente cara.

Per proteggersi da programmi di selezione non desiderati e a pagamento (dialer 0190/0900), consigliamo di rivolgersi direttamente al proprio gestore telefonico per bloccare questo tipo di numeri.

Di default, il prodotto Avira riconosce i programmi di selezione a pagamento a lui noti.

Se nella configurazione di Categorie delle minacce l'opzione **Programma di selezione a pagamento** è attivata con un segno di spunta, in caso di rilevamento di un programma di selezione a pagamento si riceve un messaggio di avviso. Si ha quindi la possibilità di eliminare facilmente gli eventuali dialer indesiderati per i numeri 0190/0900. Se si tratta di un programma di selezione a pagamento voluto, si può dichiarare un file da escludere che non verrà più scansionato in futuro.

Phishing

Il phishing, anche noto come "brand spoofing" è una forma raffinata di furto dei dati per i clienti o i potenziali clienti di provider Internet, banche, servizi di online banking, enti di registrazione.
Con la trasmissione dell'indirizzo email in Internet, la compilazione di moduli online, la partecipazione a newsgroup o siti web è possibile che vengano sottratti i dati dai cosiddetti

"Internet crawling spiders" e utilizzati senza consenso per effettuare frodi o altre attività illegali.

Il prodotto Avira riconosce il "phishing". Se nella configurazione in Categorie delle minacce l'opzione **Phishing** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira rileva un tale comportamento.

Programmi che violano la privacy dell'utente

Software che minano la sicurezza del sistema, causano funzioni di programma non desiderate, violano la sfera privata o spiano il comportamento dell'utente e che sono quindi generalmente indesiderati.

Il prodotto Avira riconosce il "software Security Privacy Risk". Se nella configurazione in Categorie delle minacce l'opzione **Programmi che violano la privacy dell'utente** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira effettua un rilevamento.

Programmi ludici

I programmi ludici possono inorridire qualcuno o divertire tutti, senza essere dannosi o moltiplicarsi. La maggior parte delle volte il computer dopo il richiamo del programma ludico inizia a far suonare una melodia o a visualizzare qualcosa di insolito sullo schermo. Esempi di programmi ludici sono le lavatrici nel drive del floppy disk (DRAIN.COM) o il divoraschermo (BUGSRES.COM).

Ma attenzione! Tutte le manifestazioni di un programma ludico potrebbero anche essere prodotte da un virus o un trojan. L'effetto minimo sull'utente è uno spavento ma si può anche andare nel panico per la paura dei danni che possono verificarsi.

Il prodotto Avira è in grado di riconoscere i programmi ludici mediante un'estensione delle proprie routine di scansione ed eventualmente di eliminare il programma indesiderato. Se nella configurazione in Categorie delle minacce l'opzione **Programmi ludici** è attivata con un segno di spunta, si viene informati sui relativi rilevamenti.

Giochi

I giochi per computer devono esistere, ma non necessariamente sul luogo di lavoro (ad eccezione a volte della pausa pranzo). Tuttavia i dipendenti delle aziende e i collaboratori degli enti pubblici spesso usano i giochi. Su Internet sono disponibili moltissimi giochi. Anche i giochi per email stanno conoscendo una rapida espansione: dai semplici scacchi fino a "battaglia navale" esistono numerose varianti: i giochi vengono inviati per email ai partner e accettati da questi ultimi.

Alcune ricerche hanno dimostrato che il tempo durante l'orario lavorativo dedicato ai giochi per computer sta assumendo proporzioni rilevanti. Pertanto è comprensibile che sempre più aziende prendano in considerazione la possibilità di eliminare i giochi dai computer utilizzati per lavoro.

Il prodotto Avira riconosce i giochi per computer. Se nella configurazione in Categorie delle minacce l'opzione **Giochi** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira effettua un rilevamento. Il gioco è finito nel vero senso della parola visto che è possibile escluderlo facilmente.

Software ingannevole

Conosciuto anche come "Scareware" (programma che fa spavento dall'inglese "to scare") o "Rogueware" (programma perfido o falso antivirus), definisce software fraudolento, che simula infezioni causate da virus e minacce, e assomiglia in modo sorprendente ai software antivirus professionali. Scareware è progettato per rendere insicuro o impaurire l'utente. La vittima cade nel trabocchetto e si crede minacciata, per cui le viene proposta, spesso a pagamento, l'eliminazione di un pericolo inesistente. In altri casi la vittima, credendo che sia avvenuto un attacco, viene indotta a intraprendere azioni che rendono possibile un'attacco vero e proprio.

Se nella configurazione di Categorie delle minacce l'opzione **Software ingannevole** è attivata con un segno di spunta, in caso di rilevamento di scareware si riceve un messaggio di avviso.

Strumento di compressione runtime insolito

I file compressi con un programma zip runtime insolito possono essere identificati come sospetti.

Il prodotto Avira riconosce "Strumento di compressione runtime insolito". Se nella configurazione in Categorie delle minacce l'opzione **Strumento di compressione runtime insolito (PCK)** è attivata, si riceve un avviso quando il prodotto Avira effettua un rilevamento.

8.2 Virus e altri malware

Adware

Con Adware si designa un software che mostra all'utente i banner e i pop up pubblicitari. Questi inserti pubblicitari generalmente non possono essere chiusi e sono quasi sempre visibili. I dati della connessione permettono numerosi feedback sul comportamento dell'utente e sono problematici per motivi di sicurezza dei dati.

Backdoor

Un Backdoor (italiano: porta posteriore) permette, aggirando la tutela all'accesso, di ottenere l'accesso a un computer.

Un programma in esecuzione di nascosto permette a un aggressore di godere di diritti pressoché illimitati. Con l'aiuto del backdoor i dati personali dell'utente possono essere

spiati. I backdoor però vengono utilizzati soprattutto per installare altri virus o worm sul sistema infetto.

Virus dei record di avvio

Il record di avvio e il record master di avvio degli hard disk vengono inficiati di preferenza da virus dei record di avvio, che sovrascrivono informazioni importanti all'avvio del sistema. Una delle conseguenze spiacevoli: il sistema operativo non può più essere caricato...

Bot-Net

Per Bot-Net si intende una rete di PC gestibile a distanza (in Internet), composta da bot che comunicano l'uno con l'altro. Questo controllo si raggiunge con virus e trojan che inficiano il computer e poi aspettano indicazioni senza apportare danni al computer intaccato. Queste reti possono essere utilizzare per la diffusione di spam, attacchi DDoS, ecc., talvolta senza che gli utenti del PC si accorgano di alcunché. Il potenziale principale dei Bot-Net è quello di poter raggiungere reti di migliaia di computer, la cui portata salta gli accessi a Internet.

Exploit

Un Exploit (lacuna di sicurezza) è un programma del computer o uno script che sfrutta le debolezze specifiche o le funzioni errate di un sistema operativo o del programma. Una forma di Exploit sono gli attacchi da Internet con l'aiuto di pacchetti di dati manipolati, che sfruttano le debolezze nel software di rete. Con l'utilizzo di alcuni programmi che si introducono clandestinamente si ottiene un più ampio accesso.

Hoaxes (inglese: hoax - scherzo, burla)

Da un paio di anni gli utenti ricevono avvisi di virus che potrebbero diffondersi per email in Internet o in altre reti. Questi avvisi vengono distribuiti per email con la richiesta di inoltrarli a quanti più colleghi e utenti possibili per metterli in guardia sul "pericolo".

Honeypot

Un Honeypot (pentola di miele) è un servizio installato in una rete (programma o server). Esso ha il compito di monitorare una rete e registrare gli attacchi. Questo servizio è sconosciuto all'utente legittimo e quindi non viene mai toccato. Quando un aggressore cerca punti di debolezza in una rete e prende in considerazione i servizi offerti da un Honeypot viene registrato e viene emesso un allarme.

Macrovirus

I macrovirus sono piccoli programmi che sono scritti nella lingua delle macro di un'applicazione (ad esempio WordBasic in WinWord 6.0) e normalmente potrebbero diffondersi all'interno di documenti di questa applicazione. Essi vengono pertanto chiamati anche virus dei documenti. Per renderli attivi è necessario avviare l'applicazione corrispondente ed eseguire una delle macro infette. Diversamente dai virus "normali" i macrovirus non riguardano file eseguibili, ma documenti dell'applicazione host.

Pharming

Il pharming è una manipolazione del file host dei browser Web, per reindirizzare richieste dei siti Web falsificati. Si tratta di una rielaborazione del classico phishing. I truffatori che si servono del pharming godono di grandi quantità di server sui quali vengono archiviati i siti Web falsificati. Il pharming si è consolidato come iperonimo per diversi tipi di attacchi al DNS. In caso di manipolazione del file host con l'ausilio di un trojan o un virus viene effettuata una manipolazione del sistema. La conseguenza è che sono richiamabili solo siti Web falsificati da questo sistema, se l'indirizzo Web viene inserito correttamente.

Phishing

Phishing significa letteralmente pescare dati personali degli utenti di Internet. Il phisher invia generalmente alla vittima lettere aventi valore ufficiale, come ad esempio email che veicolano informazioni sensibili, soprattutto nomi utenti e password o PIN e TAN di accessi all'Online-Banking, approfittando della sua buona fede. Con i dati di accesso rubati il phisher assume l'identità della vittima e conduce operazioni a suo nome. Una cosa è certa: le banche e le assicurazioni non chiedono mai di inviare numeri di carte di credito, PIN, TAN o altri dati di accesso per email, SMS o telefonicamente.

Virus polimorfi

I veri campioni del mimetismo e del travestimento sono i virus polimorfi. Modificano i codici di programmazione e sono pertanto difficili da riconoscere.

Virus di programma

Un virus del computer è un programma che ha la capacità, una volta richiamato, di agganciarsi in qualche modo ad altri programmi e, da tale posizione, di inficiare il sistema. I virus si diffondono quindi in contrasto alle bombe logiche e ai trojan stessi. Al contrario di un worm, un virus ha bisogno di un programma estraneo ospite in cui archiviare il proprio codice virulento. Normalmente, la funzionalità del programma ospite non viene modificata.

Rootkits

Per Rootkit si intende un insieme di strumenti software che vengono installati su un computer dopo un'irruzione per nascondere il login dell'intruso, nascondere processi e registrare dati - in linea generale: per rendersi invisibile. I rootkit tentano di aggiornare i programmi spia già installati e di installare nuovamente gli spyware eliminati.

Virus di script e worm

Questi virus sono estremamente semplici da programmare e in poche ore si diffondono per email a livello globale, premesso che siano presenti tecniche ad hoc.

I virus di script e i worm utilizzano la lingua degli script, come ad esempio Javascript, VBScript ecc., per inserirsi in altri nuovi script o per diffondersi mediante il richiamo di funzioni del sistema operativo. Spesso ciò avviene tramite email o mediante lo scambio di file (documenti).

Il worm è un programma che non intacca alcun documento ospite. I worm non possono quindi divenire una componente di altri programmi. I worm rappresentano spesso l'unica possibilità di introdursi clandestinamente su sistemi dotati di provvedimenti restrittivi legati alla sicurezza.

Spyware

Gli spyware sono i cosiddetti programmi spia che inviano dati personali dell'utente a terzi senza che questi ne siano a conoscenza e senza l'approvazione del produttore del software. I programmi spyware servono soprattutto ad analizzare la navigazione in Internet e a introdurre banner o pop up pubblicitari in maniera mirata.

Cavalli di Troia (in breve trojan)

I trojan sono sempre più diffusi. Così vengono definiti i programmi che pretendono di avere una funzione precisa; dopo il loro avvio, tuttavia, mostrano il loro vero volto ed eseguono altre funzioni che hanno per lo più effetti distruttivi. I trojan non possono moltiplicarsi da soli e in questo si differenziano dai virus e dai worm. La maggior parte di loro ha un nome interessante (SEX.EXE o STARTME.EXE), che ha la funzione di spingere l'utente a eseguire il trojan. Subito dopo l'esecuzione diventano attivi e formattano, ad esempio, l'hard disk. Un tipo particolare di trojan è il dropper, che "lascia cadere" i virus, ovvero li installa nel sistema del computer.

Software ingannevole

Conosciuto anche come "Scareware" (programma che fa spavento dall'inglese "to scare") o "Rogueware" (programma perfido o falso antivirus), definisce software fraudolento, che simula infezioni causate da virus e minacce, e assomiglia in modo sorprendente ai software antivirus professionali. Scareware è progettato per rendere insicuro o impaurire

l'utente. La vittima cade nel trabocchetto e si crede minacciata, per cui le viene proposta, spesso a pagamento, l'eliminazione di un pericolo inesistente. In altri casi la vittima, credendo che sia avvenuto un attacco, viene indotta a intraprendere azioni che rendono possibile un'attacco vero e proprio.

Zombie

Un PC zombie è un calcolatore che è intaccato da programmi malware e permette all'hacker di abusare del computer mediante la gestione a distanza per fini criminali. Il PC infetto lancia il comando, ad esempio, di attacchi di Denial-of-Service- (DoS) o invia spam o email di phishing.

9. Info e Service

In questo capitolo si ottengono informazioni sui modi in cui è possibile tenersi in contatto con noi.

- Vedere capitolo Indirizzo di contatto
- Vedere capitolo Supporto tecnico
- Vedere capitolo File sospetto
- Vedere capitolo Comunicare un falso allarme

9.1 Indirizzi di contatto

Siamo a disposizione del cliente qualora avesse domande o suggerimenti sul mondo dei prodotti Avira. I nostri indirizzi dove contattarci sono disponibili in Guida in linea > Informazioni su Avira Free Antivirus.

9.2 Supporto tecnico

Il supporto Avira si rivolge all'utente in modo affidabile e serve a rispondere alle sue domande o a risolvere un problema tecnico.

Sul nostro sito Web l'utente può riferire tutte le informazioni utili per il nostro ampio servizio di supporto:
http://www.avira.it/personal-support

Per poter ricevere aiuto nel modo migliore e più veloce possibile l'utente deve prendere in considerazione le seguenti informazioni:

- **Informazioni sulla versione**. Esse si trovano sull'interfaccia del programma nella voce di menu **Guida in linea > Informazioni su Avira Free Antivirus > Informazioni sulla versione**. Vedere Informazioni sulla versione.
- **Versione del sistema operativo** e service pack eventualmente installati.
- **I pacchetti software installati**, ad esempio software antivirus di altri produttori.
- **Messaggi precisi** del programma o del file di report.

9.3 File sospetto

I virus che non possono essere riconosciuti o eliminati dai nostri prodotti così come i file sospetti possono essere inviati a noi. A tale scopo sono disponibili diverse modalità di invio.

- Selezionare il file nel Gestore della quarantenadel Control Center e selezionare la voce Invia file mediante il menu contestuale o i pulsanti corrispondenti.

- Allegare il file desiderato compresso (WinZIP, PKZip, Arj, ecc.) ad un'email e inviarlo al seguente indirizzo:
  virus-personal@avira.it
  Poiché alcuni gateway email operano con software antivirus, si prega di proteggere il/i file con una password (non dimenticare di comunicare anche la password).

9.4 Comunicare un falso allarme

Se si ritiene che il proprio prodotto Avira abbia segnalato un rilevamento in un file che tuttavia con ogni probabilità è "pulito", si prega di inviare tale file compresso (WinZIP, PKZIP, Arj, ecc.) per email come allegato al seguente indirizzo:
virus-personal@avira.it

Poiché alcuni Email-Gateways operano con software antivirus, si prega di proteggere il file/i file con una password (non dimenticare di comunicare anche la password).

10. Riferimento: Opzioni di configurazione

Il riferimento della configurazione elenca le opzioni di configurazione disponibili.

10.1 System Scanner

La rubrica **System Scanner** della configurazione è dedicata alla configurazione della scansione diretta, ovvero alla scansione su richiesta. (Opzioni disponibili solo in Modalità esperto).

10.1.1 Cerca

Qui si può definire la procedura standard della routine di scansione durante una scansione diretta (opzioni disponibili solo in Modalità esperto). Se si seleziona una determinata directory da controllare durante la scansione diretta, il System Scanner esegue i controlli in base alla configurazione:

- con una determinata prestazione di scansione (priorità),
- anche sui record di avvio e nella memoria principale,
- su tutti i file o i file selezionati nella directory.

File

Il System Scanner può utilizzare un filtro per scansionare solamente i file con una determinata estensione (tipo).

Tutti i file

Se l'opzione è attivata, viene eseguita una ricerca di virus e programmi indesiderati in tutti i file, indipendentemente dal contenuto e dall'estensione. Il filtro non viene utilizzato.

> **Suggerimenti**
> Se **Tutti i file** è attivo, il pulsante **Estensioni dei file** non è selezionabile.

Utilizza estensioni smart

Se l'opzione è attivata, la selezione dei file da scansionare viene effettuata automaticamente dal programma. Ciò significa che il prodotto Avira decide in base al contenuto se un file deve essere controllato o meno per la presenza di virus e programmi indesiderati. Questa procedura è lievemente più lenta di **Utilizza lista estensione file**, ma molto più sicura poiché i controlli non sono effettuati solamente sulla base delle estensioni dei file. Questa opzione è attivata di default ed è consigliata.

> **Suggerimenti**
> Se **Utilizza estensioni smart** è attivo, il pulsante **Estensioni file** non può essere scelto.

Utilizza la lista delle estensioni

Se l'opzione è attivata, vengono scansionati solo i file con una determinata estensione. Sono preimpostati tutti i tipi di file che possono contenere virus e programmi indesiderati. L'elenco può essere modificato manualmente mediante il pulsante "**Estensioni file"**.

> **Suggerimenti**
> Se questa opzione è attivata e tutte le voci dell'elenco delle estensioni dei file sono state eliminate, viene visualizzato il testo "*Nessuna estensione dei file*" sotto il pulsante **Estensioni file**.

Estensioni file

Con questo pulsante viene richiamata una finestra di dialogo nella quale sono riportate tutte le estensioni dei file che vengono controllate durante una scansione in modalità "**Utilizza elenco estensioni file"**. Tra le estensioni sono presenti voci standard, ma è possibile anche aggiungere o eliminare voci.

> **Suggerimenti**
> Prestare attenzione al fatto che l'elenco standard può variare da versione a versione.

Impostazioni aggiuntive

Scansiona settori di avvio dei drive

Se l'opzione è attivata, il System Scanner controlla i record di avvio dei drive selezionati durante la scansione diretta. Questa opzione è attivata di default.

Scansione dei record master di avvio

Se l'opzione è attivata, il System Scanner controlla i record master di avvio degli/dell'hard disk utilizzati/o nel sistema.

Ignora i file offline

Se l'opzione è attivata, durante la scansione diretta i cosiddetti file offline vengono completamente ignorati. Ciò significa che in questi file non viene controllata la presenza di virus e programmi indesiderati. I file offline sono quei file che sono stati archiviati fisicamente dall'hard disk, per es. su un nastro, mediante il cosiddetto sistema gerarchico di gestione della memoria. Questa opzione è attivata di default.

Controllo di integrità dei file di sistema

Se l'opzione è attivata, i principali file di sistema Windows vengono sottoposti a una verifica particolarmente sicura durante ogni scansione diretta per verificare la presenza di modifiche dovute a malware. Se viene individuato un file modificato, questo viene segnalato come rilevamento sospetto. La funzionalità occupa molta memoria. Per questo motivo l'opzione è disattivata di default.

Suggerimenti
L'opzione è disponibile solo a partire da Windows Vista.

Suggerimenti
Se si utilizzano strumenti di terzi, si modificano i file di sistema o si personalizza la schermata di avvio, questa opzione non deve essere utilizzata. Questi strumenti sono, ad esempio, i cosiddetti skinpack, TuneUp Utilities o Vista Customization.

Scansione ottimizzata

Se l'opzione è attivata, la capacità del processore viene utilizzata in modo ottimale durante la scansione con il System Scanner. Per motivi di performance, in caso di scansione ottimale, la funzione di report si verifica al massimo a un livello standard.

Suggerimenti
L'opzione è disponibile solo per computer multiprocessore,

Seguire link simbolici

Se l'opzione è attivata, il System Scanner esegue una scansione di tutti i collegamenti simbolici nel profilo di ricerca o nelle directory selezionate, allo scopo di scansionare i file collegati alla ricerca di virus e malware.

Suggerimenti
L'opzione non comprende i collegamenti (shortcut), bensì si riferisce esclusivamente ai link simbolici (generati con mklink.exe) o ai punti di giunzione (generati con junction.exe), presenti in modalità trasparente nel file system.

Scansione rootkit all'avvio

Se l'opzione è attivata, il System Scanner verifica con una scansione all'avvio la directory di sistema Windows tramite una procedura rapida per verificare la presenza di eventuali rootkit attivi. Questa procedura non verifica se nel computer vi sono rootkit

attivi così dettagliatamente come il profilo di ricerca "**Cerca rootkit**", ma è molto più rapida.

Suggerimenti
La scansione rootkit non è disponibile in Windows XP 64 Bit!

Scansiona registro

Se l'opzione è attivata, viene scansionato il registro alla ricerca di software dannosi.

Processo di scansione

Permetti di arrestare sist. di scansione

Se l'opzione è attivata, la ricerca di virus o programmi indesiderati può essere arrestata in ogni momento con il pulsante "**Arresta"** nella finestra "**Luke Filewalker**". Se questa impostazione è disattivata, il pulsante **Arresta** nella finestra "**Luke Filewalker**" è grigio. Pertanto non è possibile terminare prematuramente una scansione! Questa opzione è attivata di default.

Priorità del sistema di scansione

Il System Scanner differenzia tre livelli di priorità nella scansione diretta. Si tratta di un sistema efficace solo se sul computer sono in esecuzione più processi contemporaneamente. La scelta si ripercuote anche sulla velocità di scansione.

basso

Il System Scanner riceve dal sistema operativo il tempo del processore solo se nessun altro processo necessita di tempo di elaborazione, ovvero finché il System Scanner è l'unico programma in esecuzione, la velocità è massima. Nel complesso, in questo modo viene gestito molto bene anche il lavoro con altri programmi: Il computer è più veloce se altri programmi sono in esecuzione, mentre il System Scanner lavora in background.

medio

Il System Scanner viene eseguito con priorità normale. Tutti i processi ricevono lo stesso tempo di elaborazione dal sistema operativo. Questa opzione è attivata di default ed è consigliata. In alcune circostanze il lavoro con altre applicazioni ne risulta compromesso.

elevato

Il System Scanner riceve la massima priorità. Un lavoro parallelo con altre applicazioni è pressoché impossibile. Tuttavia il System Scanner effettua la scansione in maniera estremamente rapida.

Azione per i rilevamenti

È possibile stabilire delle azioni che System Scanner deve eseguire quando viene rilevato un virus o un programma indesiderato. (Opzioni disponibili solo in Modalità esperto)

Interattivo

Se l'opzione è attivata, i rilevamenti della scansione del System Scanner vengono notificati in una finestra di dialogo. Al termine della scansione, si riceve un avviso con l'elenco dei file infetti rilevati. Mediante il menu contestuale è possibile selezionare un'azione da eseguire per i singoli file infetti. È possibile eseguire l'azione selezionata per tutti i file infetti oppure interrompere la scansione di System Scanner.

> **Suggerimenti**
> Di default nella finestra di dialogo è preselezionata l'azione **Quarantena**. È possibile selezionare ulteriori azioni mediante il menu contestuale.

Automatico

Se l'opzione è attivata, in caso di rilevamento di un virus o di programmi indesiderati non appare alcuna finestra di dialogo in cui selezionare l'azione da eseguire. Il System Scanner reagisce conformemente alle impostazioni effettuate precedentemente dall'utente in questa sezione.

Backup in quarantena

Se l'opzione è attivata, il System Scanner crea una copia di sicurezza (backup) prima dell'esecuzione delle azioni primarie e secondarie desiderate. La copia di sicurezza viene mantenuta in quarantena dove il file può essere ripristinato se possiede un valore informativo. Inoltre è possibile inviare la copia di sicurezza ad Avira Malware Research Center per ulteriori indagini.

Azione primaria

L'azione primaria è l'azione che viene eseguita quando il System Scanner rileva un virus o un programma indesiderato. Se l'opzione "**Ripara"** è attiva, ma la riparazione del file infetto non è possibile, verrà eseguita l'azione definita in "**Azione secondaria"**.

> **Suggerimenti**
> L'opzione **Azione secondaria** è selezionabile solo se in **Azione primaria** è stata selezionata l'impostazione **Ripara**.

Ripara

Se l'opzione è attivata, il System Scanner ripara automaticamente i file infetti. Se il System Scanner non può riparare un file infetto, in alternativa esegue l'opzione selezionata in Azione secondaria.

Suggerimenti
Si consiglia una riparazione automatica, che tuttavia comporta una modifica dei file presenti sul computer da parte del System Scanner.

Rinomina

Se l'opzione è attivata, il System Scanner rinomina il file. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere riparati successivamente e nuovamente rinominati.

quarantena

Se l'opzione è attivata, il System Scanner sposta il file in quarantena. I file possono essere riparati successivamente o, se necessario, inviati ad Avira Malware Research Center.

Elimina

Se l'opzione è attivata, il file viene eliminato.

Ignora

Se l'opzione è attivata, l'accesso al file viene consentito e il file viene mantenuto.

Attenzione
Il file infetto rimane attivo sul computer! Questo potrebbe causare danni notevoli al computer!

Azione secondaria

L'opzione "**Azione secondaria"** è selezionabile solo se in "**Azione primaria"** è stata selezionata l'impostazione **Ripara**. Con questa opzione si può decidere cosa fare con il file infetto se non è riparabile.

Rinomina

Se l'opzione è attivata, il System Scanner rinomina il file. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere riparati successivamente e nuovamente rinominati.

quarantena

Se l'opzione è attivata, il System Scanner sposta il file in quarantena. I file possono essere riparati successivamente o, se necessario, inviati ad Avira Malware Research Center.

Elimina

Se l'opzione è attiva, il file viene eliminato.

Ignora

Se l'opzione è attivata, l'accesso al file viene consentito e il file viene mantenuto.

Attenzione
Il file infetto rimane attivo sul computer! Questo potrebbe causare danni notevoli al computer!

Suggerimenti
Se si seleziona **Elimina** o come azione principale o secondaria, attenersi alle seguenti indicazioni: in caso di rilevamento di oggetti euristici, i file infetti non vengono eliminati, bensì spostati in quarantena.

Archivi

Per la ricerca negli archivi il System Scanner utilizza una scansione ricorsiva: vengono decompressi anche gli archivi in altri archivi e viene controllata la presenza di virus e programmi indesiderati. I file compressi vengono scansionati, decompressi e nuovamente scansionati. (Opzioni disponibili solo in Modalità esperto).

Scansiona archivi

Se l'opzione è attivata, vengono scansionati gli archivi selezionati nell'elenco degli archivi. Questa opzione è attivata di default.

Tutti i tipi di archivio

Se l'opzione è attivata, vengono selezionati e scansionati i tipi di archivi nella lista di archivi.

Smart Extension

Se l'opzione è attivata, il System Scanner riconosce se un file è in formato compresso (archivio), anche se l'estensione è diversa da quelle abituali, e scansiona l'archivio. Tuttavia a tal fine ogni file deve essere aperto, riducendo così la velocità della scansione. Esempio: se un archivio *.zip ha estensione *.xyz, il System Scanner decomprime anche tale archivio e lo scansiona. Questa opzione è attivata di default.

Suggerimenti
Vengono scansionati solo quei tipi di archivio che sono selezionati nell'elenco degli archivi.

Limita la profondità di ricorsione

La decompressione e la scansione di archivi particolarmente ramificati può necessitare di molto tempo e molte risorse del sistema. Se l'opzione è attivata, è possibile limitare la profondità della scansione in archivi multipli a un determinato numero di livelli di compressione (profondità di ricorsione massima). In questo modo è possibile risparmiare tempo e risorse del processore.

Suggerimenti
Per individuare un virus o un programma indesiderato all'interno di un archivio, il System Scanner deve eseguire la scansione fino al livello di ricorsione nel quale si trova il virus o il programma indesiderato.

Profondità massima di ricorsione

Per poter indicare la profondità massima di ricorsione l'opzione **Limita profondità di ricorsione** deve essere attivato.
È possibile inserire direttamente la profondità di ricorsione desiderata oppure modificarla per mezzo dei tasti freccia a destra del campo. I valori consentiti sono compresi tra 1 e 99. Il valore standard e consigliato è 20.

Valori predefiniti

Il pulsante crea i valori predefiniti per la scansione degli archivi.

Elenco archivi

In questa sezione è possibile impostare quali archivi devono essere scansionati dal System Scanner. A tal fine è necessario attivare le voci corrispondenti.

Eccezioni

Oggetti file da escludere dalla scansione (Opzioni disponibili solo in Modalità esperto).

L'elenco in questa finestra contiene file e percorsi che non devono essere presi in considerazione dal System Scanner durante la ricerca di virus e programmi indesiderati.

Si consiglia di inserire quante meno eccezioni possibili e solo i file che non devono essere scansionati durante una scansione normale per qualsivoglia motivo. Consigliamo di far comunque controllare la presenza di virus o programmi indesiderati in questi file prima di inserirli in questo elenco!

Suggerimenti
Le voci dell'elenco non possono superare complessivamente i 6000 caratteri.

Attenzione
Questi file non vengono presi in considerazione durante la scansione!

Suggerimenti
I file inseriti in questa lista vengono segnalati nel file di report. Controllare di tanto in tanto nel file di report la presenza di questi file non scansionati poiché potrebbe non sussistere più il motivo per il quale sono stati esclusi. In questo caso i nomi di questi file dovrebbero essere eliminati dall'elenco.

Campo

Inserire in questo campo il nome del file che non deve essere preso in considerazione durante una scansione diretta. Di default non è indicato alcun file.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare il file o il percorso desiderato.
Se si è fornito un nome di file con un percorso completo, tale file non viene scansionato. Se si è inserito un nome di file senza un percorso, ogni file con tale nome (indipendentemente dal percorso o dal drive) non verrà scansionato.

Aggiungi

Con il pulsante è possibile accettare il file indicato nel campo nella finestra di visualizzazione.

Elimina

Il pulsante elimina una voce selezionata nella lista. Questo pulsante non è attivo se non è selezionata alcuna voce.

> **Suggerimenti**
> Se si aggiunge un'intera partizione all'elenco dei file da escludere, verranno tralasciati dalla scansione solo i file salvati direttamente nella partizione e non i file contenuti in directory all'interno della partizione:
> Esempio: file da omettere: `D:\ = D:\file.txt` viene escluso dalla scansione del System Scanner, `D:\folder\file.txt` viene incluso nella scansione.

Euristico

Questa rubrica di configurazione contiene le impostazioni per l'euristica del motore di ricerca. (Opzioni disponibili solo in Modalità esperto).

I prodotti Avira contengono un'euristica molto efficace, che consente di riconoscere in modo proattivo malware sconosciuti, ovvero prima che venga creata una firma speciale dei virus contro il parassita e che venga inviato un aggiornamento della protezione antivirus. Il riconoscimento dei virus avviene attraverso un'approfondita analisi e indagine del relativo codice in base alle funzioni tipiche dei malware. Se il codice esaminato corrisponde a tali caratteristiche tipiche viene segnalato come sospetto. Ciò non significa necessariamente che il codice indichi effettivamente la presenza di un malware; potrebbe trattarsi anche di messaggi di errore. La decisione su come procedere con il codice spetta all'utente stesso, ad esempio sulla base delle sue conoscenze relativamente all'attendibilità della fonte che contiene il codice segnalato.

Macrovirus euristico

Macrovirus euristico

Il prodotto Avira acquistato contiene un macrovirus euristico molto efficace. Se l'opzione è attivata, in caso di riparazione possibile tutte le macro del documento infetto vengono eliminate, in alternativa i documenti sospetti vengono solo segnalati, l'utente riceverà quindi un avviso. Questa impostazione è attivata di default e viene consigliata.

Advanced Heuristic Analysis and Detection (AHeAD)

Attiva AHeAD

Il programma Avira contiene, grazie alla tecnologia Avira AHeAD, un'euristica molto efficace, in grado di riconoscere anche malware sconosciuti (nuovi). Se l'opzione è attivata, è possibile impostare il grado di rigidità dell'euristica. Questa opzione è attivata di default.

Livello di rilevamento basso

Se l'opzione è attivata, viene riconosciuto un numero inferiore di malware sconosciuti e il rischio di possibili rilevamenti di errore è limitato.

Livello di rilevamento medio

Questa impostazione è attivata di default, se è stata scelta l'applicazione di questa euristica.

Livello di riconoscimento elevato

Se l'opzione è attivata, viene riconosciuto un numero significativamente maggiore di malware sconosciuti, ma possono verificarsi messaggi di errore.

10.1.2 Report

Il System Scanner possiede una funzione di log molto ampia. In questo modo si ricevono informazioni esatte sui risultati di una scansione diretta. Il file di report contiene tutte le voci del sistema e gli avvisi e i messaggi della scansione diretta. (Opzioni disponibili solo in Modalità esperto.)

Suggerimenti
Per comprendere quali azioni il System Scanner ha eseguito in caso di rilevamento di virus o programmi indesiderati, deve sempre essere creato un file di report.

Funzione di log

Disabilitato

Se l'opzione è attivata, il System Scanner non riporta le azioni e i risultati della scansione diretta.

Standard

Se l'opzione è attivata, il System Scanner riporta il nome dei file infetti con il percorso. Inoltre, la configurazione per la scansione attuale, le informazioni sulla versione e sul proprietario della licenza viene riportata nel file di report.

Avanzato

Se l'opzione è attivata, il System Scanner riporta anche gli avvisi e le note, oltre alle informazioni standard.

Completo

Se l'opzione è attivata, il System Scanner riporta tutti i file scansionati. Inoltre, tutti i file infetti, nonché gli avvisi e le note vengono registrati nel file di report.

Suggerimenti
Se l'utente deve inviare un file di report ad Avira (per la ricerca dell'errore), preghiamo di creare il file di report con questa modalità.

10.2 Realtime Protection

La rubrica Realtime Protection della configurazione è dedicata alla configurazione di Realtime Protection. (Opzioni disponibili solo in Modalità esperto).

10.2.1 Cerca

Solitamente si desidera che il proprio sistema sia costantemente monitorato. Per questo viene utilizzato Realtime Protection (scansione in tempo reale = On-Access Scanner). In questo modo è possibile ricercare la presenza di virus e programmi indesiderati in tutti i file che vengono aperti o copiati sul computer "on the fly". (Opzione disponibile solo in Modalità esperto).

File

Realtime Protection può utilizzare un filtro per scansionare solamente i file con una determinata estensione (tipo).

Tutti i file

Se l'opzione è attivata, viene eseguita una ricerca di virus e programmi indesiderati in tutti i file, indipendentemente dal contenuto e dall'estensione.

Suggerimenti
Se **Tutti i file** è attivo, il pulsante **Estensioni dei file** non è selezionabile.

Utilizza estensioni smart

Se l'opzione è attivata, la selezione dei file da scansionare viene effettuata automaticamente dal programma. Ciò significa che il programma decide in base al contenuto se un file deve essere controllato o meno per la presenza di virus e programmi indesiderati. Questa procedura è lievemente più lenta di **Utilizza lista estensione file**, ma molto più sicura poiché i controlli non sono effettuati solamente sulla base delle estensioni dei file.

> **Suggerimenti**
> Se **Utilizza estensioni smart** è attivo, il pulsante **Estensioni file** non può essere scelto.

Utilizza la lista delle estensioni

Se l'opzione è attivata, vengono scansionati solo i file con una determinata estensione. Sono preimpostati tutti i tipi di file che possono contenere virus e programmi indesiderati. L'elenco può essere modificato manualmente mediante il pulsante "**Estensioni file"**. Questa opzione è attivata di default ed è consigliata.

> **Suggerimenti**
> Se questa opzione è attivata e tutte le voci dell'elenco delle estensioni dei file sono state eliminate, viene visualizzato il testo "*Nessuna estensione dei file*" sotto il pulsante **Estensioni file**.

Estensioni file

Con questo pulsante viene richiamata una finestra di dialogo nella quale sono riportate tutte le estensioni dei file che vengono controllate durante una scansione in modalità "**Utilizza elenco estensioni file"**. Tra le estensioni sono presenti voci standard, ma è possibile anche aggiungere o eliminare voci.

> **Suggerimenti**
> Prestare attenzione al fatto che l'elenco estensioni dei file può variare da versione a versione.

Modalità di scansione

Qui si stabilisce il momento in cui effettuare la scansione di un file.

Scansione in lettura

Se l'opzione è attivata, Realtime Protection scansiona i file prima che vengano letti o eseguiti da un'applicazione o dal sistema operativo.

Scansione in scrittura

Se l'opzione è attivata, Realtime Protection scansiona un file in scrittura. Dopo questa procedura è possibile accedere nuovamente al file.

Scansione in lettura e scrittura

Se l'opzione è attivata, Realtime Protection scansiona i file prima dell'apertura, della lettura e dell'esecuzione e dopo la scrittura. Questa impostazione è attivata di default e viene consigliata.

Archivi

Scansiona archivi

Se l'opzione è attivata, vengono scansionati gli archivi. I file compressi vengono scansionati, decompressi e nuovamente scansionati. Questa opzione è disattivata di default. La scansione degli archivi viene limitata dalla profondità di ricorsione, dal numero di file da scansionare e dalle dimensioni dell'archivio. È possibile impostare la profondità di ricorsione, il numero di file da scansionare e le dimensioni massime dell'archivio.

Suggerimenti
L'opzione è disattivata di default poiché il processo occupa molta memoria. Generalmente si consiglia di scansionare gli archivi con la scansione diretta.

Profondità massima di ricorsione

Per la ricerca negli archivi, Realtime Protection utilizza una scansione ricorsiva: vengono decompressi anche gli archivi in altri archivi e viene controllata la presenza di virus e programmi indesiderati. L'utente può stabilire la profondità di ricorsione. Il valore standard per la profondità di ricorsione è 1 ed è quello consigliato: tutti i file che si trovano direttamente nell'archivio principale vengono scansionati.

Numero max. di file

Per la ricerca negli archivi la scansione viene limitata a un numero massimo di file dell'archivio. Il valore standard per il numero massimo di file da scansionare è 10 e viene consigliato.

Dimensione max. (KB)

Per la ricerca negli archivi la scansione viene limitata a una dimensione degli archivi massima, da decomprimere. Il valore standard è 1000 KB ed è consigliato.

Azione per i rilevamenti

Utilizza il log degli eventi

Se l'opzione è attivata, viene inserita una voce nel log eventi di Windows a ogni rilevamento. È possibile richiamare gli eventi nel visualizzatore eventi di Windows. Questa opzione è attivata di default. (Opzione disponibile solo in Modalità esperto).

Eccezioni

Con queste opzioni è possibile configurare gli oggetti soggetti a eccezioni per Realtime Protection (scansione in tempo reale). Gli oggetti identificati verranno così esclusi dalla scansione in tempo reale. Realtime Protection può ignorare gli accessi ai file riportati nell'elenco dei processi da tralasciare durante la scansione in tempo reale. Questa funzione è utile ad esempio per le banche dati o le soluzioni di backup. (Opzioni disponibili solo in Modalità esperto).

Nell'indicare i processi e gli oggetti file da escludere, prestare attenzione a quanto segue: L'elenco viene elaborato dall'alto verso il basso. Più lungo è l'elenco, maggiore è il tempo di cui il processore ha bisogno per elaborare l'elenco a ogni accesso. Si consiglia pertanto di mantenere l'elenco più breve possibile.

Processi esclusi da Realtime Protection

Tutti gli accessi ai file dei processi indicati in questo elenco sono stati esclusi dal monitoraggio mediante Realtime Protection.

Campo

Inserire in questo campo il nome del processo che deve essere ignorato dalla scansione in tempo reale. Di default non è indicato alcun processo.

Il percorso indicato e il nome del file del processo non possono superare i 255 caratteri. È possibile inserire fino a 128 processi. Le voci dell'elenco non possono superare complessivamente i 6000 caratteri.

Pr indicare i processi è possibile utilizzare caratteri Unicode. Pertanto, è possibile indicare nomi di processi o directory che contengono caratteri speciali.

I drive devono essere indicati nel modo seguente: `[Laufwerksbuchstabe]:\`

Il simbolo dei due punti (:) deve essere utilizzato solo per indicare il drive.

Per indicare il processo, è possibile utilizzare la wildcard * (numero a piacere di caratteri) e ? (un unico carattere):

```
C:\Programme\Anwendung\anwendung.exe
C:\Programme\Anwendung\anwendun?.exe
C:\Programme\Anwendung\anwend*.exe
C:\Programme\Anwendung\*.exe
```

Per evitare che l'intero processo venga escluso dal monitoraggio di Realtime Protection, i dati che contengono esclusivamente i seguenti caratteri non sono validi: * (asterisco), ? (punto interrogativo), / (barra), \ (barra rovesciata), . (punto), : (due punti).

È possibile escludere dal monitoraggio di Realtime Protection i processi senza percorso completo: `anwendung.exe`

Ciò è valido solo per i processi i cui file eseguibili si trovano sul drive dell'hard disk.

Non indicare alcuna eccezione per i processi i cui file eseguibili si trovano su drive dinamici. I drive dinamici vengono utilizzati per i supporti dati rimovibili, quali CD, DVD o penna USB.

Attenzione
Prestare attenzione al fatto che tutti gli accessi ai file dei processi che sono stati evidenziati nell'elenco sono esclusi dalla scansione di virus e programmi indesiderati! Esplora risorse di Windows e il sistema operativo non possono essere esclusi. La voce corrispondente nell'elenco viene ignorata.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare un file eseguibile.

Processi

Il pulsante "**Processi"** apre la finestra "*Selezione del processo"*, in cui vengono indicati i processi in corso.

Aggiungi

Con il pulsante è possibile è possibile accettare il processo indicato nella finestra di visualizzazione.

Elimina

Con il pulsante si elimina un processo selezionato dalla finestra di visualizzazione.

Oggetti file da escludere da Realtime Protection

Tutti gli accessi ai file degli oggetti indicati in questo elenco sono esclusi dal monitoraggio mediante Realtime Protection.

Campo

Inserire in questo campo il nome del file che deve essere ignorato dalla scansione in tempo reale. Di default non è indicato alcun file.

Le voci dell'elenco non possono superare complessivamente i 6000 caratteri.

Per indicare i file da omettere, è possibile utilizzare la wildcard * (numero a piacere di caratteri) e ? (un unico carattere). È possibile anche escludere singole estensioni di file (incluse le wildcard):

```
C:\Verzeichnis\*.mdb
*.mdb
*.md?
*.xls*
C:\Verzeichnis\*.log
```

VI nomi delle directory devono concludersi con una barra inversa \, altrimenti viene confuso con un nome di file.

Se una directory viene esclusa, anche tutte le sottodirectory che contiene vengono escluse automaticamente.

Per ogni drive è possibile indicare al massimo 20 eccezioni con il percorso completo (che inizia con la lettera del drive).

Es.: `C:\Programme\Anwendung\Name.log`

Il numero massimo di eccezioni senza percorso completo è 64. Es.:

`*.log`

In caso di drive dinamici, collegati (montati) come directory a un altro drive, è necessario utilizzare nell'elenco delle eccezioni il nome dell'alias del sistema operativo per il drive collegato:
ad es. `\Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\`
Anche utilizzando il punto di montaggio stesso (mount point), ad es. `C:\DynDrive`, si esegue comunque la scansione del drive dinamico. È possibile ricavare i nomi dell'alias del sistema operativo da utilizzare dal file di report di Realtime Protection.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare i file da tralasciare.

Aggiungi

Con il pulsante è possibile accettare il file indicato nel campo nella finestra di visualizzazione.

Elimina

Con il pulsante si elimina un file selezionato dalla finestra di visualizzazione.

Per indicare le eccezioni, attenersi alle seguenti indicazioni

Per escludere oggetti anche quando vi si accede con nomi di file DOS brevi (convenzione dei nomi di DOS 8.3), è necessario inserire nell'elenco il nome breve del file corrispondente.

Un nome di file che contiene wildcard non deve concludersi con una barra inversa.
Ad esempio:
`C:\Programme\Anwendung\anwend*.exe\`
Questa voce non è valida e non viene considerata come un'eccezione!

In base al file di report di Realtime Protection è possibile ricavare i percorsi utilizzati da Realtime Protection durante la ricerca dei file infetti. Nell'elenco delle eccezioni, utilizzare di massima gli stessi percorsi. Procedere come segue: impostare la funzione di log di Realtime Protection nella configurazione in Report su **Completo**. Quindi accedere con

Realtime Protection attivato a file, directory, drive collegati. È ora possibile leggere il percorso da utilizzare dal file di report di Realtime Protection. È possibile richiamare il file di report nel Control Center in Realtime Protection.

Euristico

Questa rubrica di configurazione contiene le impostazioni per l'euristica del motore di ricerca. (Opzione disponibile solo in Modalità esperto).

I prodotti Avira contengono un'euristica molto efficace, che consente di riconoscere in modo proattivo malware sconosciuti, ovvero prima che venga creata una firma speciale dei virus contro il parassita e che venga inviato un aggiornamento della protezione antivirus. Il riconoscimento dei virus avviene attraverso un'approfondita analisi e indagine del relativo codice in base alle funzioni tipiche dei malware. Se il codice esaminato corrisponde a tali caratteristiche tipiche viene segnalato come sospetto. Ciò non significa necessariamente che il codice indichi effettivamente la presenza di un malware; potrebbe trattarsi anche di messaggi di errore. La decisione su come procedere con il codice spetta all'utente stesso, ad esempio sulla base delle sue conoscenze relativamente all'attendibilità della fonte che contiene il codice segnalato.

Macrovirus euristico

Macrovirus euristico

Il prodotto Avira acquistato contiene un macrovirus euristico molto efficace. Se l'opzione è attivata, in caso di riparazione possibile tutte le macro del documento infetto vengono eliminate, in alternativa i documenti sospetti vengono solo segnalati, l'utente riceverà quindi un avviso. Questa impostazione è attivata di default e viene consigliata.

Advanced Heuristic Analysis and Detection (AHeAD)

Attiva AHeAD

Il programma Avira contiene, grazie alla tecnologia Avira AHeAD, un'euristica molto efficace, in grado di riconoscere anche malware sconosciuti (nuovi). Se l'opzione è attivata, è possibile impostare il grado di rigidità dell'euristica. Questa opzione è attivata di default.

Livello di rilevamento basso

Se l'opzione è attivata, viene riconosciuto un numero inferiore di malware sconosciuti e il rischio di possibili rilevamenti di errore è limitato.

Livello di rilevamento medio

Questa impostazione è attivata di default, se è stata scelta l'applicazione di questa euristica.

Livello di riconoscimento elevato

Se l'opzione è attivata, viene riconosciuto un numero significativamente maggiore di malware sconosciuti, ma possono verificarsi messaggi di errore.

10.2.2 Report

Realtime Protection possiede una funzione di log molto vasta che può fornire all'utente o all'amministratore informazioni esatte sulla modalità di un rilevamento. " ?> (Opzione disponibile solo in Modalità esperto).

Funzione di log

In questo gruppo viene definita la portata contenutistica del file di report.

Disabilitato

Se l'opzione è attivata, Realtime Protection non crea alcun protocollo.
In casi eccezionali si può rinunciare alla funzione di report, solo se si eseguono test con molti virus o programmi indesiderati.

Standard

Se l'opzione è attivata, Realtime Protection registra informazioni importanti (su rilevamenti, avvisi ed errori) nel file di report, mentre le informazioni meno importanti vengono ignorate per maggiore chiarezza. Questa opzione è attivata di default.

Avanzato

Se l'opzione è attivata, Realtime Protection registra nel file di report anche le informazioni meno importanti.

Completo

Se l'opzione è attivata, Realtime Protection registra tutte le informazioni - anche quelle relative alla dimensione del file, al tipo, alla data, ecc. - nel file di report.

Limitazioni del file di report

Limita la dimensione a n MB

Se l'opzione è attivata, il file di report può essere limitato a una determinata dimensione; valori possibili: da 1 a 100 MB. Con la limitazione del file di report si introduce un intervallo di circa 50 kilobyte per non sovraccaricare il processore. Se la dimensione del file di report supera la dimensione indicata di 50 kilobyte, vengono automaticamente eliminate le voci meno recenti fin quando si raggiunge una dimensione inferiore a 50 kilobyte.

Backup file report prima della limitazione

Se l'opzione è attivata il file del report viene salvato prima dell'abbreviazione.

Scrivi la configurazione nel file di report

Se l'opzione è attivata, la configurazione utilizzata della scansione in tempo reale viene riportata nel file di report.

Suggerimenti
Se non sono state specificate limitazioni per i file di report, viene creato un nuovo file di report quando questo raggiunge le dimensioni di 100 MB. Viene creato un backup del report di dati precedente. Vengono mantenuti fino a tre backup di report di dati precedenti. Vengono eliminati di volta in volta i backup meno recenti.

10.3 Aggiornamento

Nella rubrica **Aggiornamento** configurare l'esecuzione automatica degli aggiornamenti. È possibile impostare diversi intervalli di aggiornamento.

Aggiornamento automatico

ogni n giorno/i / ora/e / minuto/i

In questo campo è possibile indicare l'intervallo in cui devono essere eseguiti gli aggiornamenti automatici. Per modificare l'intervallo di aggiornamento, è possibile indicare un dato temporale nel campo e modificarlo mediante i tasti freccia a destra del campo.

Ripeti job se il tempo è scaduto

Se l'opzione è attivata, vengono eseguiti job di aggiornamento scaduti che non è stato possibile eseguire al momento designato, ad esempio perché il computer era spento. (Opzione disponibile solo in Modalità esperto).

10.3.1 Aggiornamento di prodotto

In **Aggiornamento prodotto** configurare l'esecuzione degli aggiornamenti del prodotto o la notifica della disponibilità di tali aggiornamenti. (Opzioni disponibili solo in Modalità esperto).

Aggiornamenti prodotto

Scarica aggiornamenti del prodotto e installa automaticamente

Se l'opzione è attivata, gli aggiornamenti del prodotto vengono scaricati e installati automaticamente, non appena si rendono disponibili, dai componenti di aggiornamento. Gli aggiornamenti del file di definizione dei virus e del motore di ricerca avvengono sempre e indipendentemente da questa impostazione. Le premesse per utilizzare questa opzione sono: configurazione completa dell'aggiornamento e collegamento esistente a un server di download.

Scaricare aggiornamenti del prodotto. Se è necessario riavviare, installare l'aggiornamento dopo il successivo riavvio del sistema, altrimenti eseguire immediatamente l'installazione.

Se l'opzione è attivata, gli aggiornamenti del prodotto vengono scaricati non appena disponibili. L'aggiornamento viene installato automaticamente dopo il download dei file di aggiornamento, qualora non sia necessario il riavvio. Se si tratta di un aggiornamento del prodotto che richiede il riavvio del computer, tale aggiornamento non viene eseguito subito dopo il download dei file di aggiornamento, bensì solo dopo il successivo riavvio del sistema effettuato dall'utente. Il vantaggio che ne deriva è che il riavvio non viene eseguito mentre l'utente sta lavorando al computer. Gli aggiornamenti del file di definizione dei virus e del motore di ricerca avvengono sempre e indipendentemente da questa impostazione. Le premesse per utilizzare questa opzione sono: configurazione completa dell'aggiornamento e collegamento esistente a un server di download.

Avvisa quando sono disponibili nuovi aggiornamenti del prodotto

Se l'opzione è attivata, si viene avvisati solo se sono disponibili nuovi aggiornamenti per il prodotto. Gli aggiornamenti del file di definizione dei virus e del motore di ricerca avvengono sempre e indipendentemente da questa impostazione. Le premesse per utilizzare questa opzione sono: configurazione completa dell'aggiornamento e collegamento esistente a un server di download.La notifica avviene tramite un messaggio sul desktop sotto forma di una finestra di pop up e tramite un avviso dell'Updater nel Control Center in Panoramica > Eventi.

Avvisa nuovamente dopo n giorno(i)

Indicare in questo campo dopo quanti giorni si desidera ricevere nuovamente la notifica relativa alla disponibilità degli aggiornamenti del prodotto, qualora l'aggiornamento del prodotto non sia stato eseguito alla prima notifica.

Non scaricare aggiornamenti prodotto

Se l'opzione è attivata, non si effettuano aggiornamenti automatici o notifiche se sono disponibili aggiornamenti del prodotto mediante l'Updater. Gli aggiornamenti del file delle definizioni dei virus e del motore di ricerca avvengono sempre indipendentemente da questa impostazione.

Attenzione
L'aggiornamento del file di definizione dei virus e del motore di ricerca avviene contestualmente a ogni aggiornamento effettuato, indipendentemente dalle impostazioni per l'aggiornamento di prodotto (vedere Aggiornamenti).

Suggerimenti
Se è stata attivata l'opzione per l'aggiornamento automatico del prodotto, è possibile configurare ulteriori opzioni di notifica e possibilità di interruzione del riavvio in Impostazioni riavvio. (Opzioni disponibili solo in Modalità esperto).

10.3.2 Riavvio impostazioni

Quando viene eseguito un aggiornamento del prodotto Avira, può essere necessario un riavvio del sistema. Se è stata impostata un'esecuzione automatica dell'aggiornamento del prodotto in Aggiornamento > Aggiornamento prodotto, è possibile scegliere fra diverse opzioni di notifica e per l'interruzione del riavvio in **Impostazioni riavvio**. (Opzioni disponibili solo in Modalità esperto).

Suggerimenti
Nell'effettuare le impostazioni di riavvio, si noti che nella configurazione è possibile scegliere fra due opzioni per l'esecuzione degli aggiornamenti del prodotto con riavvio necessario del computer, in Aggiornamento > Aggiornamento prodotto:
- **Scarica aggiornamenti del prodotto e installa automaticamente**: L'aggiornamento e il riavvio vengono eseguiti quando l'utente sta utilizzando il computer. Se è stata attivata questa opzione, possono essere utili le routine di riavvio con possibilità di interruzione oppure con funzione di avviso.
- **Scaricare aggiornamenti del prodotto. Se è necessario riavviare, installare l'aggiornamento dopo il successivo riavvio del sistema, altrimenti eseguire immediatamente l'installazione**: l'aggiornamento e il riavvio vengono eseguiti dopo che l'utente ha avviato il computer e si è registrato. Per questa opzione sono consigliabili le routine di riavvio automatiche.

Riavvio del sistema dopo n secondi (con conto alla rovescia, nessuna possibilità di interruzione)

Se l'opzione è attivata, il riavvio necessario viene eseguito **automaticamente** dopo l'esecuzione di un aggiornamento del prodotto secondo l'intervallo di tempo indicato. Compare un conto alla rovescia, senza possibilità di interrompere il riavvio del sistema.

Ricordo periodico di riavvio

Se l'opzione è attivata, il riavvio necessario **non viene eseguito automaticamente** dopo un aggiornamento del prodotto. Nell'intervallo di tempo indicato, vengono visualizzati avvisi di riavvio senza possibilità di interruzione. Negli avvisi è possibile confermare il riavvio del sistema oppure selezionare l'opzione "**Ricorda ancora"**.

Richiesta di esecuzione di riavvio del sistema

Se l'opzione è attivata, il riavvio necessario **non viene eseguito automaticamente** dopo un aggiornamento del prodotto. Viene visualizzato una sola volta un messaggio in cui è possibile confermare il riavvio oppure interrompere la routine di riavvio.

Riavvio del sistema senza richiesta

Se l'opzione è attivata, il riavvio necessario viene eseguito **automaticamente** dopo un aggiornamento del prodotto. Non si riceve alcun messaggio.

10.3.3 Server web

Server web

L'aggiornamento può essere eseguito direttamente mediante server web in Internet. (Opzioni disponibili solo in Modalità esperto).

Connessione al server Web

Utilizza una connessione esistente (rete)

Questa impostazione viene visualizzata se viene utilizzata la connessione mediante una rete.

Utilizzare la seguente connessione:

Questa impostazione viene visualizzata se si definisce individualmente la connessione.

L'Updater riconosce automaticamente quali opzioni di connessione sono disponibili. Le opzioni di connessione non disponibili sono grigie e non possono essere attivate. Ad esempio, è possibile creare manualmente una connessione dial-up mediante una voce dell'elenco telefonico di Windows.

Utente

inserire il nome utente dell'account selezionato.

Password

inserire la password per questo account. Per ragioni di sicurezza i caratteri effettivi che si inseriscono nel campo vengono visualizzati come asterischi (*).

Suggerimenti
Se sono stati dimenticati il nome utente o la password di un account Internet contattare il provider di servizi Internet.

Suggerimenti
La selezione automatica dell'Updater mediante i cosiddetti strumenti dial-up (ad esempio SmartSurfer, Oleco, ...) attualmente non è ancora disponibile.

Termina la connessione dial-up al termine dell'aggiornamento

Se l'opzione è attivata, viene interrotta automaticamente la connessione dial-up aperta per l'aggiornamento, non appena il download è stato eseguito con successo.

Suggerimenti
L'opzione non è disponibile in Vista e in Windows 7. In Vista e in Windows 7 la

connessione dial-up, aperta per l'aggiornamento, viene sempre interrotta, non appena il download è stato eseguito.

Impostazioni proxy

Proxyserver

Non utilizzare un server Proxy

Se l'opzione è attivata, la connessione al server web viene effettuata mediante un server proxy.

Utilizza impostazioni di sistema di Windows

Se l'opzione è attivata, vengono utilizzate le impostazioni di sistema di Windows correnti per la connessione al server Web mediante un server proxy. Per configurare le impostazioni di sistema di Windows per l'utilizzo di un server proxy, accedere a **Pannello di controllo > Opzioni Internet > Connessioni > Impostazioni LAN**. È possibile accedere alle opzioni Internet anche nel menu **Extra** di Internet Explorer.

Attenzione
Quando si utilizza un server proxy che richiede l'autenticazione, immettere tutti i dati tramite l'opzione **Utilizza questo server proxy**. Per i server proxy senza autenticazione, è possibile utilizzare l'opzione **Utilizza impostazioni di sistema di Windows**.

Utilizza questo server proxy

Se l'opzione è attivata, la connessione al server web avviene mediante un server proxy, utilizzando le impostazioni definite.

Indirizzo

Immettere il nome computer o l'indirizzo IP del server proxy che si desidera utilizzare per la connessione al server Web.

Porta

Immettere il numero della porta del server proxy che si desidera utilizzare per la connessione al server Web.

Nome Login

Immettere un nome utente per la registrazione sul server proxy.

Password

Inserire la password appropriata per la registrazione sul server proxy. Per ragioni di sicurezza i caratteri effettivi che si inseriscono nel campo vengono visualizzati come asterischi (*).

Esempi:

Indirizzo: `proxy.domain.de` Porta: `8080`

Indirizzo: `192.168.1.100` Porta: `3128`

10.4 Web Protection

La rubrica **Web Protection** in **Configurazione > Sicurezza Internet** è dedicata alla configurazione di Web Protection.

10.4.1 Cerca

Web Protection consente di proteggersi da virus e malware, che giungono sul computer attraverso i siti Web caricati da Internet nel browser Web. Nella rubrica **Scansione** è possibile impostare il comportamento di Web Protection. (Opzioni disponibili solo in Modalità esperto).

Cerca

Supporto di IPv6

Se l'opzione è attivata, viene supportata la versione 6 di Web Protection.

Protezione drive-by

La *protezione drive-by* consente di effettuare impostazioni per bloccare gli iframe, detti anche inline frame. Gli iframe sono elementi HTML, ovvero elementi di siti Internet, che delimitano un'area di un sito Web. Gli iframe consentono di caricare e visualizzare altri contenuti Web, per lo più di altri URL, come documenti indipendenti in una sottofinestra del browser. Gli iframe vengono principalmente utilizzati per i banner pubblicitari. In alcuni casi gli iframe vengono utilizzati per nascondere virus e malware. In questi casi l'area dell'iframe nel browser è appena o per niente visibile. L'opzione **Blocca iframe sospetti** consente di controllare e di bloccare il caricamento di iframe.

Blocca I-Frames sospetti

Se l'opzione è attivata, gli iframe dei siti richiesti vengono verificati in base a determinati criteri. Se in uno dei siti Web richiesti sono presenti iframe sospetti, l'iframe viene bloccato. Nella finestra dell'iframe viene visualizzato un messaggio di errore.

Azione per i rilevamenti

È possibile stabilire delle azioni che Web Protection deve eseguire quando viene rilevato un virus o un programma indesiderato. (Opzioni disponibili solo in Modalità esperto.)

Interattivo

Se l'opzione è attivata, durante la scansione diretta in caso di rilevamento di un virus o di un programma indesiderato, viene visualizzata una finestra di dialogo nella quale è

possibile scegliere come procedere con i file infetti. Questa opzione è attivata di default.

Visualizza barra di progressione

Se l'opzione è attivata, quando un download o lo scaricamento del contenuto di pagine Websupera un timeout di 20 secondi viene visualizzato un messaggio sul desktop con una barra di progressione per il download. Questo messaggio sul desktop è utile in particolare per il controllo del download da pagine Web con grandi volumi di dati: navigando con Web Protection i contenuti delle pagine Web non vengono caricati gradualmente nel browser Internet poiché, prima di essere visualizzati nel browser Internet vengono scansionati alla ricerca di virus e malware. Questa opzione è disattivata di default.

É possibile reperire maggiori informazioni qui.

Automatico

Se l'opzione è attivata, in caso di rilevamento di un virus o di programmi indesiderati non appare alcuna finestra di dialogo in cui selezionare l'azione da eseguire. Web Protection reagisce conformemente alle impostazioni effettuate dall'utente in questa sezione.

Azione primaria

L'azione primaria è l'azione che viene eseguita quando Web Protection rileva un virus o un programma indesiderato.

Nega accesso

Il sito Web richiesto dal server Web o i dati e i file trasferiti non vengono inviati al proprio browser Web. Nel browser Web viene visualizzato un messaggio di errore relativo al divieto di accesso. Web Protection inserisce il rilevamento nel file di report, a condizione che la funzione di report sia attivata.

quarantena

Il sito Web richiesto dal server Web o i dati e i file trasferiti vengono inviati in quarantena in caso di rilevamento di un virus o di un malware. Il file infetto può essere ripristinato dal Gestore della quarantena se ha un valore informativo, oppure, se necessario, inviato ad Avira Malware Research Center.

Ignora

Il sito Web richiesto dal server Web o i dati e i file trasferiti vengono inoltrati da Web Protection al proprio browser Web. L'accesso al file viene consentito e il file viene mantenuto.

> **Attenzione**
> Il file infetto rimane attivo sul computer! Questo potrebbe causare danni notevoli al computer!

Accessi bloccati

Il filtro Web consente di bloccare URL noti indesiderati, quali gli URL di phishing e malware. Web Protection impedisce il trasferimento dei file da Internet al computer. (Opzioni disponibili solo in Modalità esperto).

Filtro Web

Il filtro Web dispone di una banca dati interna aggiornata quotidianamente nella quale gli URL sono classificati in base a criteri di contenuto.

Attiva filtro Web

Se l'opzione è attivata, vengono bloccati tutti gli URL appartenenti alle categorie selezionate nell'elenco del filtro Web.

Elenco filtro Web

Nell'elenco del filtro Web è possibile selezionare le categorie di contenuto i cui URL devono essere bloccati da Web Protection.

Suggerimenti
Il filtro web viene ignorato per le voci dell'elenco degli URL da tralasciare in Eccezioni.

Suggerimenti
Vengono categorizzati come**URL di spam** gli URL diffusi con i messaggi email di spam. La categoria **Frode/Inganno** comprende i siti web con 'abbonamenti-trappola' e altre offerte di servizi i cui costi vengono occultati dal fornitore.

Eccezioni

Queste opzioni consentono di escludere tipi di MIME (tipi di contenuto dei file trasferiti) e tipi di file per gli URL (indirizzi Internet) dalla scansione di Web Protection. Gli URL e i tipi di MIME indicati vengono ignorati da Web Protection, ovvero durante la trasmissione al computer dell'utente non viene effettuata la scansione di questi dati per verificare la presenza di virus e malware (opzioni disponibili solo in Modalità esperto).

Tipi di MIME da omettere da Web Protection

In questo campo è possibile selezionare tipi di MIME (tipi di contenuto dei dati trasferiti) che devono essere esclusi dalla scansione di Web Protection.

Tipi di file / tipi di MIME da escludere da Web Protection (definiti dall'utente)

Tutti i tipi di file e i tipi di MIME (tipi di contenuto dei dati trasferiti) nell'elenco vengono esclusi dalla scansione di Web Protection.

Campo

Inserire in questo campo i nomi dei tipi di MIME e di file che si intendono escludere dalla scansione di Web Protection. Per i tipi di file, inserire l'estensione del file, ad esempio `.htm`. Per i MIME segnalare il tipo di supporto ed eventualmente il sottotipo. I due dati vengono separati da una semplice barra, ad esempio`video/mpeg` oppure `audio/x-wav`.

Suggerimenti
Nell'immissione dei tipi di file e di MIME non è possibile utilizzare wildcard (wildcard * per un numero a piacere di caratteri o ? per un solo carattere).

Attenzione
Tutti i tipi di file e di contenuto nell'elenco delle eccezioni vengono caricati nel browser Internet senza ulteriori verifiche : Non viene eseguita alcuna scansione per virus e malware.

Tipi di MIME: esempi per tipi di supporto

- `text` per file di testo
- `image` = per file di grafica
- `video` = per file video
- `audio` = per file audio
- `application` = per file associati a un programma specifico

Esempi: tipi di file e di MIME da escludere

- `audio/` = tutti i file del tipo di supporto audio vengono esclusi dalla scansione di Web Protection
- `video/quicktime` = tutti i file video del sottotipo Quicktime (*.qt, *.mov) vengono esclusi dalla scansione di Web Protection
- `.pdf` = tutti i file Adobe-PDF vengono esclusi dalla scansione di Web Protection.

Aggiungi

Con il pulsante è possibile accettare i MIME e il tipo di file indicati nella finestra.

Elimina

Il pulsante elimina una voce selezionata nella lista. Questo pulsante non è attivo se non è selezionata alcuna voce.

URL da omettere da Web Protection

Tutti gli URL di questo elenco vengono esclusi dalla scansione di Web Protection.

Campo

Immettere in questo campo gli URL (indirizzi Internet) che devono essere esclusi dalla scansione di Web Protection, ad es.**www.domainname.com**. È possibile inserire parti di URL definendo il livello del dominio con punti iniziali o finali: .domainname.it per tutte le pagine e i tutti i domini secondari del dominio. Per indicare una pagina Web con un dominio di livello superiore a piacere (.com o .net), utilizzare un punto finale: **domainname.**. Se si utilizza una sequenza di caratteri senza punto iniziale o finale, viene interpretata come dominio di livello superiore, ad es. **net** per tutti i domini NET (www.domain.net).

Suggerimenti
Nell'immissione degli URL è possibile utilizzare anche wildcard * per un numero di caratteri a piacere. Per definire il livello del dominio, utilizzare anche punti iniziali o finali in combinazione con wildcard:
`.domainname.*`
`*.domainname.com`
`.*name*.com` (valido ma non consigliato)
I dati senza punti quali `*name*` vengono interpretati come parti di dominio di livello superiore e non sono consigliati.

Attenzione
Tutte le pagine web dell'elenco degli URL da escludere vengono caricati nel browser Internet senza ulteriori verifiche del filtro Web o di Web Protection : per tutte le voci dell'elenco degli URL da tralasciare vengono ignorate le voci del filtro Web (vedere Accesso bloccato). Non viene eseguita alcuna scansione per virus e malware. Si consiglia pertanto di escludere dalla scansione di Web Protection solo URL affidabili.

Aggiungi

Con il pulsante è possibile accettare nella finestra gli URL (indirizzi Internet) indicati.

Elimina

Il pulsante elimina una voce selezionata nella lista. Questo pulsante non è attivo se non è selezionata alcuna voce.

Esempi: URL da tralasciare

- `www.avira.com` -O- `www.avira.com/*`
  = Tutti gli URL con dominio 'www.avira.com' vengono esclusi dalla scansione di Web Protection: www.avira.com/en/pages/index.php, www.avira.com/en/support/index.html, www.avira.com/en/download/index.html,..
  Gli URL con dominio www.avira.com/it vengono esclusi dalla scansione di Web Protection.

- `avira.com` -O- `*.avira.com`
  = Tutti gli URL con dominio di livello secondario o superiore 'avira.com' vengono esclusi dalla scansione di Web Protection. Tali dati comprendono tutti i domini secondari esistenti di '.avira.com': www.avira.com, forum.avira.com,...
- `avira.` -O- `*.avira.*`
  = Tutti gli URL con dominio di livello secondario 'avira' vengono esclusi dalla scansione di Web Protection. Tali dati comprendono tutti i domini esistenti di livello superiore o i domini secondari di '.avira.': www.avira.com, www.avira.com/it, forum.avira.com,...
- `.*domain*.*`
  = Tutti gli URL che contengono un dominio di livello secondario con la sequenza di caratteri 'domain', vengono esclusi dalla scansione di Web Protection: www.domain.com, www.new-domain.it, www.sample-domain1.it, ...
- `net` -O- `*.net`
  = Tutti gli URL con dominio di livello superiore 'net' vengono esclusi dalla scansione di Web Protection: www.name1.net, www.name2.net,...

> **Attenzione**
> Indicare tutti gli URL che si desidera escludere dalla scansione di Web Protection nel modo più preciso possibile. Evitare l'immissione di tutti i domini di livello superiore o parti di nomi di domini secondari, poiché vi è il rischio che le pagine Internet, che diffondono malware e programmi indesiderati mediante dati globali, vengano escluse dalla scansione di Web Protection come eccezione. Si consiglia di immettere almeno il dominio secondario e il dominio di livello superiore completi: domainname.com

Euristico

Questa rubrica di configurazione contiene le impostazioni per l'euristica del motore di ricerca. (Opzioni disponibili solo in Modalità esperto).

I prodotti Avira contengono un'euristica molto efficace, che consente di riconoscere in modo proattivo malware sconosciuti, ovvero prima che venga creata una firma speciale dei virus contro il parassita e che venga inviato un aggiornamento della protezione antivirus. Il riconoscimento dei virus avviene attraverso un'approfondita analisi e indagine del relativo codice in base alle funzioni tipiche dei malware. Se il codice esaminato corrisponde a tali caratteristiche tipiche viene segnalato come sospetto. Ciò non significa necessariamente che il codice indichi effettivamente la presenza di un malware; potrebbe trattarsi anche di messaggi di errore. La decisione su come procedere con il codice spetta all'utente stesso, ad esempio sulla base delle sue conoscenze relativamente all'attendibilità della fonte che contiene il codice segnalato.

Macrovirus euristico

Il prodotto Avira acquistato contiene un macrovirus euristico molto efficace. Se l'opzione è attivata, in caso di riparazione possibile tutte le macro del documento infetto vengono eliminate, in alternativa i documenti sospetti vengono solo segnalati,

l'utente riceverà quindi un avviso. Questa impostazione è attivata di default e viene consigliata.

Advanced Heuristic Analysis and Detection (AHeAD)

Attiva AHeAD

Il prodotto Avira contiene, grazie alla tecnologia Avira AHeAD, un'euristica molto efficace, in grado di riconoscere anche malware sconosciuti (nuovi). Se l'opzione è attivata, è possibile impostare il grado di rigidità dell'euristica. Questa opzione è attivata di default.

Livello di rilevamento basso

Se l'opzione è attivata, viene riconosciuto un numero inferiore di malware sconosciuti e il rischio di possibili rilevamenti di errore è limitato.

Livello di rilevamento medio

Questa impostazione è attivata di default, se è stata scelta l'applicazione di questa euristica.

Livello di riconoscimento elevato

Se l'opzione è attivata, viene riconosciuto un numero significativamente maggiore di malware sconosciuti, ma possono verificarsi messaggi di errore.

10.4.2 Report

Web Protection possiede una funzione di log molto vasta che può fornire all'utente o all'amministratore informazioni esatte sulla modalità di un rilevamento.

Funzione di log

In questo gruppo viene definita la portata contenutistica del file di report.

Disabilitato

Se l'opzione è attivata, Web Protection non crea alcun protocollo.
In casi eccezionali si può rinunciare alla funzione di report, solo se si eseguono test con molti virus o programmi indesiderati.

Standard

Se l'opzione è attivata, Web Protection registra informazioni importanti (su rilevamenti, avvisi ed errori) nel file di report, mentre le informazioni meno importanti vengono ignorate per maggiore chiarezza. Questa opzione è attivata di default.

Avanzato

Se l'opzione è attivata, Web Protection registra nel file di report anche le informazioni meno importanti.

Completo

Se l'opzione è attivata, Web Protection registra tutte le informazioni - anche quelle relative alla dimensione del file, al tipo, alla data, ecc. - nel file di report.

Limitazioni del file di report

Limita la dimensione a n MB

Se l'opzione è attivata, il file di report può essere limitato a una determinata dimensione; valori possibili: da 1 a 100 MB. Con la limitazione del file di report si introduce un intervallo di circa 50 kilobyte per non sovraccaricare il processore. Se la dimensione del file di report supera la dimensione fissata di 50 Kilobyte, vengono automaticamente eliminate le voci più vecchie fin quando non si raggiunge una dimensione inferiore del 20%.

Scrivi la configurazione nel file di report

Se l'opzione è attivata, la configurazione utilizzata della scansione in tempo reale viene riportata nel file di report.

Suggerimenti
Se non sono state specificate limitazioni per i file di report, vengono automaticamente eliminate le voci più vecchie quando il file di report raggiunge le dimensioni di 100 MB. Viene eliminato un numero di voci tali da consentire al file di report di raggiungere una dimensione di 80 MB.

10.5 Generale

10.5.1 Categorie di minacce

Selezione delle categorie estese delle minacce (Opzioni disponibili solo in Modalità esperto).

Il prodotto Avira protegge dai virus del computer. Inoltre, si ha la possibilità di effettuare una scansione differenziata in base alle seguenti categorie delle minacce.

- Adware
- Adware/Spyware
- Applicazioni
- Software di controllo backdoor
- File con estensioni nascoste
- Programma di selezione a pagamento
- Phishing
- Programmi che violano la privacy dell'utente

- Programmi ludici
- Giochi
- Software ingannevole
- Strumento di compressione runtime insolito

Facendo clic sulla casella appropriata viene attivata (spuntata) o disattivata (non spuntata) la modalità selezionata.

Attiva tutti

Se l'opzione è attivata vengono attivate tutte le modalità.

Valori predefiniti

Questo pulsante ripristina i valori standard predefiniti.

Suggerimenti
Se viene disattivata una modalità, i file riconosciuti come tale tipo di programma non verranno più segnalati. Non viene riportata alcuna segnalazione nemmeno sul file di report.

10.5.2 Sicurezza

Opzioni disponibili solo in Modalità esperto.

Avvio automatico

Blocca avvio automatico

Se l'opzione è attivata, l'avvio automatico di Windows viene bloccato su tutti i drive collegati, come penne USB, CD e DVD, drive di rete. Con la funzione di avvio automatico di Windows, i file sui supporti informatici o sui drive di rete vengono letti immediatamente al momento dell'inserimento o del collegamento; in questo modo i file possono essere avviati e riprodotti automaticamente. Tuttavia questa funzionalità nasconde un rischio per la sicurezza molto elevato, poiché con l'avvio automatico dei file è possibile che vengano installati malware e programmi indesiderati. Particolarmente critica è la funzione di avvio automatico delle penne USB poiché su questi supporti i file possono modificarsi continuamente.

Escludi CD e DVD

Se l'opzione è attivata, è consentita la funzione di avvio automatico sui drive CD e DVD.

Attenzione
Disattivare la funzione di avvio automatico per i drive CD e DVD solo se si è sicuri che si tratti di supporti informatici assolutamente affidabili.

Protezione del sistema

Proteggi il file host di windows da modifiche

Se questa opzione è attivata, i file host di Windows sono protetti dalla scrittura. Non è più possibile manipolare i file. Il malware non è più, ad esempio, in grado di deviare l'utente su pagine Internet indesiderate. Questa opzione è attivata di default.

Tutela del prodotto

> **Suggerimenti**
> **Le opzioni per la tutela del prodotto non sono disponibili se Realtime Protection non è stato installato in modo personalizzato.**

Proteggi i processi da una chiusura indesiderata

Se l'opzione è attivata, tutti i processi del programma vengono protetti da chiusura indesiderata dovuta a virus e malware o a una chiusura involontaria di un utente, ad esempio mediante il Task Manager. Questa opzione è attivata di default.

Protezione del processo avanzata

Se l'opzione è attivata, tutti i processi del programma vengono protetti da chiusura indesiderata con metodi avanzati. La protezione avanzata del processo consuma molte più risorse rispetto alla protezione di processo base. L'opzione è attivata di default. Per disattivare l'opzione è necessario riavviare il computer.

> **Suggerimenti**
> Protezione del processo in Windows XP 64 Bitnon disponibile!

> **Attenzione**
> Se la protezione del processo è attivata, possono verificarsi problemi di interazione con altri software. In tal caso disattivare la protezione del processo.

Proteggi i file e le voci di registrazione dalla manipolazione

Se l'opzione è attivata, tutte le voci del registro del programma e tutti i dati del programma (file binari e di configurazione) vengono protetti da manipolazione. La protezione da manipolazione comprende la protezione da interventi di scrittura, eliminazione e talvolta di lettura sulle voci del registro o sui file di programma da parte di utenti o di programmi estranei. Per attivare l'opzione è necessario riavviare il computer.

Attenzione
Si noti che, se l'opzione è disattivata, la riparazione dei computer colpiti da alcuni tipi di malware può fallire.

Suggerimenti
Se l'opzione è attivata, è possibile effettuare modifiche della configurazione o di job di scansione e aggiornamento solo tramite l'interfaccia utente.

Suggerimenti
Protezione dei file e delle voci di registrazione in Windows XP 64 Bitnon disponibile!

10.5.3 WMI

Opzioni disponibili solo in Modalità esperto.

Assistenza per Windows Management Instrumentation (WMI)

Windows Management Instrumentation è una tecnologia di gestione fondamentale di Windows che consente, mediante linguaggi di script e di programmazione in lettura e in scrittura, di accedere in locale e in remoto alle impostazioni dei computer Windows. Il prodotto Avira supporta WMI e rende disponibili dati (informazioni sullo stato, statistiche, rapporti, job pianificati ecc.), eventitramite un'interfaccia. Tramite WMI è possibile richiamare dati operativi del programma.

attiva supporto WMI

Se l'opzione è attivata, è possibile richiamare i dati operativi del programma tramite WMI.

10.5.4 Eventi

Opzioni disponibili solo in Modalità esperto.

Limitare l'estensione della banca dati degli eventi

Limita l'estensione ad un massimo di n immissioni

Se l'opzione è attiva, il numero massimo delle immissioni nella banca dati degli eventi è limitato a un preciso numero; i valori consentiti sono: da 100 a 10.000 immissioni. Se il numero delle immissioni viene superato gli inserimenti più vecchi vengono eliminati.

Elimina tutti gli eventi più vecchi di n giorno/i

Se l'opzione è attiva dopo un numero determinato di giorni gli eventi vengono eliminati dalla banca dati degli eventi; i valori consentiti sono: da 1 a 90 giorni. Di default questa opzione è attivata con un valore di 30 giorni.

Nessun limite

Con l'opzione attivata, le dimensioni della banca dati degli eventi non sono limitate. Sull'interfaccia del programma, alla voce Eventi, viene però visualizzato un massimo di 20.000 immissioni.

10.5.5 Report

Opzioni disponibili solo in Modalità esperto.

Limita i report

Limita il numero a un massimo di n pezzi

Se l'opzione è attiva, il numero massimo di report può essere limitato; i valori consentiti sono: da 1 a 300. Se il numero indicato viene superato, i report più vecchi vengono eliminati.

Elimina tutti i report più vecchi di n giorni

Se l'opzione è attiva i report vengono automaticamente eliminati dopo un determinato numero di giorni; i valori consentiti sono: da 1 a 90 giorni. Di default questa opzione è attivata con un valore di 30 giorni.

Nessun limite

Se l'opzione è attiva, il numero di report non è limitato.

10.5.6 Directory

Opzioni disponibili solo in Modalità esperto.

Percorso temporaneo

Utilizza le impostazioni predefinite

Se l'opzione è attivata vengono utilizzate le impostazioni del sistema per la gestione dei file temporanei.

> **Suggerimenti**
> I file temporanei nel sistema sono memorizzati ad esempio in Windows XP - in: **Start > Impostazioni > Pannello di controllo > Sistema >** Scheda "**Avanzate**" > Pulsanti "**Variabili d'ambiente**". Le variabili temporanee (`TEMP`,

TMP) per l'utente di volta in volta registrato e per le variabili di sistema (TEMP, TMP) sono visibili qui con i loro rispettivi valori.

Utilizza la seguente directory

Se l'opzione è attivata viene utilizzato il percorso visualizzato nel campo.

Campo

In questo campo inserire il percorso in cui i file temporanei del programma dovranno essere salvati.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare il percorso temporaneo desiderato.

Standard

Il pulsante crea la directory predefinita per il percorso temporaneo.

10.5.7 Avviso acustico

Opzioni disponibili solo in Modalità esperto.

In caso di rilevamento di un virus o di un malware tramite System Scanner o Realtime Protection viene emesso un avviso acustico in modalità di azione interattiva. È possibile attivare o disattivare l'avviso acustico oppure selezionare un file wave alternativo come avviso acustico.

Suggerimenti
La modalità di azione di System Scanner viene impostata nella configurazione in **System Scanner > Scansione > Azione in caso di rilevamento**.

Nessun avviso

Se l'opzione è attivata, non viene emesso alcun avviso acustico in caso di rilevamento tramite System Scanner o Realtime Protection.

Emetti tramite casse PC (solo in modalità interattiva)

Se l'opzione è attivata, viene emesso un avviso acustico con suono standard in caso di rilevamento di un virus tramite System Scanner o Realtime Protection. L'avviso acustico viene emesso tramite l'altoparlante interno del PC.

Utilizza il seguente file WAVE (solo in modalità interattiva)

Se l'opzione è attivata, in caso di rilevamento di un virus tramite System Scanner o Realtime Protection viene emesso un avviso acustico con il file wave selezionato. Il file wave selezionato viene riprodotto tramite un altoparlante collegato esternamente.

File wave

In questo campo è possibile inserire il nome e il percorso corrispondente di un file audio. L'avviso acustico standard del programma viene immesso di default.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare il file desiderato grazie all'explorer dei file.

Test

Questo pulsante serve a testare il file wave selezionato.

10.5.8 Avvisi

Il prodotto Avira, in caso di determinati eventi, genera messaggi sul desktop, i cosiddetti messaggi a tendina, per informare l'utente di eventuali pericoli o della riuscita o meno dell'esecuzione di un dato programma come, per esempio, un aggiornamento. È possibile attivare o disattivare in **Avvisi** la funzione di notifica per specifici eventi.

Nel caso delle notifiche sul desktop è possibile disattivare direttamente le notifiche sul messaggio a tendina. È possibile annullare la disattivazione della notifica nella finestra di configurazione **Avvisi**.

Aggiornamento

Avviso se l'aggiornamento risale a più di n giorni fa

In questo campo, è possibile inserire il numero massimo di giorni che possono trascorrere dall'ultimo aggiornamento. Se si supera questo periodo, il Control Center visualizzerà sotto Stato un'icona rossa per lo stato dell'aggiornamento.

Avvisa se il file VDF non è aggiornato

Se l'opzione è attivata, si riceve un avviso in caso di file di definizione dei virus non aggiornato. Grazie all'opzione "Avviso, se l'ultimo aggiornamento risale a più di n giorni fa", è possibile configurare un intervallo temporale.

Avvisi/indicazione nelle seguenti situazioni

Utilizzo di una connessione dial-up

Se l'opzione è attivata, l'utente è avvisato con una notifica sul desktop quando un programma di selezione stabilisce una connessione sul computer tramite la rete telefonica o ISDN. In caso di programmi di selezione esiste il rischio che si tratti di un dialer sconosciuto e indesiderato, che stabilisce una connessione a pagamento. (vedere Categorie di minacce: Dialer)

File aggiornati correttamente

Se l'opzione è attivata, l'utente riceve un messaggio sul desktop quando è stato completato con successo un aggiornamento e sono stati aggiornati file.

Aggiornamento non riuscito

Se l'opzione è attivata, l'utente riceve un messaggio sul desktop quando un aggiornamento non è stato completato con successo: Non è stato possibile stabilire una connessione con il server di download o non è stato possibile installare i file aggiornati.

Non sono necessari aggiornamenti

Se l'opzione è attivata, l'utente riceve un messaggio sul desktop quando è stato lanciato un aggiornamento ma non era necessario installare alcun file perché il programma era già aggiornato.